COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail.

Luxembourg, 19 December 2008

To all the professionals of the financial sector subject to the supervision of the CSSF and to which the law of 12 November 2004 on the fight against money laundering and terrorist financing as amended applies

CIRCULAR CSSF 08/387

Re: **Fight against money laundering and terrorist financing and prevention of the use of the financial sector for the purpose of money laundering and terrorist financing**

to be read jointly with circular CSSF 10/476 and circular CSSF 11/528

SUMMARY

Introduction

I. Development of the legislative and regulatory framework

1. Since the law of 7 July 1989 had, for the first time in Luxembourg Law, introduced the laundering of the proceeds of an illegal activity, namely drug trafficking, as a specific criminal offence, and since circular IML 89/57 had specified the rules to be observed by the professionals of the financial sector in order to prevent them from being used for the purpose of money laundering, the Luxembourg laws and regulations concerning money laundering have been strengthened continually.
At first, the law of 5 April 1993 on the financial sector implementing Community Directive 91/308/EEC and the Financial Action Task Force ("FATF") recommendations published in 1990 defined a certain number of professional obligations to be observed by the professionals of the financial sector in order to prevent them from being used for the purpose of money laundering.
Then, circular IML 94/112, which repealed circular IML 89/57, provided guidance and detailed instructions on how the professionals of the financial sector are supposed to observe the professional obligations imposed upon them by law, based notably on the above provisions of the law of 5 April 1993.

Since then, the anti-money laundering framework has developed considerably both at international and national level.

At international level, it is worth mentioning the first revision of the 40 recommendations of the FATF in 1996, the extension of the fight against money laundering to terrorist financing by means of the FATF special recommendations in October 2001, the adoption of Directive 2001/97/EC in December 2001, amending aforesaid Directive 91/308/EEC and finally the second review of the 40 FATF recommendations in June 2003.
At national level, reference must be made to the law of 11 August 1998 which, among other things, extended the scope of the money-laundering offence, the law of 12 August 2003 on the repression of terrorism and its financing, as well as the law of 12 November 2004, implementing Directive 2001/97/EC, while supplementing and strengthening the Luxembourg legislative framework on a certain number of items in the light of the experience gained in the course of the previous years in combating money laundering at international and domestic level.

These developments required the Commission de surveillance du secteur financier ("CSSF") to supplement the reference circular IML 94/112 with numerous circulars whose purpose was either to amend or to specify certain points.

Circular CSSF 05/211 dated 13 October 2005 was then introduced in order to integrate, in a consistent manner in a single circular, all the guidelines and instructions regarding the practical application of the professional obligations in order to make the existing regulation more comprehensible.
Furthermore, it adapted the existing, precise and detailed guidelines and instructions on how the professionals of the financial sector are supposed to observe the professional obligations

imposed upon them by law in order to prevent them from being used for the purposes of money laundering and terrorist financing, by taking into account the changes as well as the experience gained.

2. The constant evolution of the regulatory framework as regards the fight against money laundering and terrorist financing then led to the adoption of several European Community texts which directly impact the regulations applicable to professionals supervised by the CSSF:

- Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;
- Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC as regards the definition of "politically exposed person" and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis;
- Regulation (EC) No 1781/2006 of 15 November 2006 relating to the information on the payer accompanying transfers of funds, in order to improve the protection of payment systems against the flow of dirty money.

The aforementioned Directives, based largely on the 40 FATF recommendations which were substantially modified and developed in 2003, were transposed into Luxembourg law by a law dated 17 July 2008 transposing said Directives and amending the law of 12 November 2004 on the fight against money laundering and terrorist financing. This law modified Article 39 of the law of 5 April 1993 on the financial sector, as amended, by adapting the references to the new applicable provisions and Regulation 1781/2006 of 15 November 2006 relating to the information on the payer accompanying transfers of funds as regards wire transfers.

A second law dated the same day, the law of 17 July 2008, also concerning the fight against money laundering and financing of terrorism yet dealing predominantly with criminal matters, amended Article 506-1 of the code of criminal procedure in order to ensure compliance by the Luxembourg framework with international obligations as regards the definition of money laundering.

This Circular, which replaces Circular 05/211 of 13 October 2005, is a result of the regulatory developments described above.

The important points of the new regulation as regards the fight against money laundering and terrorist financing, already partially anticipated in Circular 05/211 and set out in detail below, can be summarised as follows:

- Introduction of a general risk-based approach: given the fact that the risk of money laundering or terrorist financing is not always the same, it is important that the professionals concentrate principally on those clients and situations which represent a real risk of money laundering or terrorist financing. On this basis, the new legislation

introduces standard customer due diligence measures which the professionals must systematically apply but the extent of which may be determined on a risk-sensitive basis. The law of 17 July 2008 further sets out a limited number of specific cases where simplified customer due diligence measures are sufficient. Finally, there are situations in which the professionals have to perform enhanced customer due diligence over and above the standard measures when there is a higher risk of money laundering or terrorist financing: this is the case in situations deemed as such by the professionals and in several specific cases expressly covered by the law where the risk of money laundering or terrorist financing is particularly high.

- Specific provisions regarding customer identification and detailed definitions of certain concepts such as “beneficial owner” and “politically exposed person”;

- Detailed description of the customer identification procedure;

- The use of specific third parties in the customer identification procedure;

- A major innovation introduced in the context of the new legislation deals with the new manner of determining third countries recognised as having a framework as regards the fight against money laundering and terrorist financing which is equivalent to that laid down by the law of 12 November 2004 as amended by the law of 17 July 2008. Further to an agreement between Member States, a common list of third countries which have an equivalent system in the fight against money laundering and terrorist financing was drawn up. This list was made compulsory in Luxembourg by way of the Grand–ducal Regulation of 29 July 2008 establishing the list of “third countries which impose equivalent requirements” within the meaning of the law of 12 November 2004 on the fight against money laundering and terrorist financing as amended (Memorial A n° 119 of 11.08.2008, p. 1811) (Annexe I). It should be noted that the list includes those countries currently considered as having an equivalent framework. This list is therefore subject to amendment, particularly on the basis of public assessment reports adopted by the FATF, regional organisations such as the FATF, the International Monetary Fund or the World Bank, reports drawn up on the basis of the FATF Recommendations and a common assessment methodology.

  In this context, it is useful to mention the meaning of « third country” according to Article 1(4) and (5) of the law of 12 November 2004 as amended: a state other than a Member State of the European Union or the European Economic Area. Contrary to third countries which are only considered equivalent if they appear on the list mentioned above, the Member States of the European Union and of the European Economic Area are equivalent as of right.

II. Persons responsible as regards the fight against money laundering and terrorist financing

3. The legally authorised managers are responsible for guaranteeing compliance with the legal and regulatory provisions, establishing, in accordance with the provisions laid down in point 122 and following of this Circular, internal anti-money laundering and terrorist financing policies and procedures and ensuring their proper implementation.
As regards specifically the internal organisation, they shall establish adequate procedures of internal control and communication in order to forestall and prevent the carrying out of operations related to money laundering or terrorist financing, including acceptance, identification and monitoring procedures as well as risk management.
They must also define the human and technical resources needed to reach these objectives.
Without prejudice to the above-mentioned managers' own responsibility, they must appoint an anti-money laundering and terrorist financing officer.
As far as credit institutions and investment firms are concerned, this person shall be the compliance officer. In accordance with Circular CSSF 04/155 relating to the compliance function, the compliance officer shall notably see to it that the professional of the financial sector has set up rules regarding the fight against money laundering and terrorist financing and that the professional complies with these rules. Furthermore, this person acts as contact person for the relevant competent authorities and, in particular, this person is in charge of reporting suspicious transactions to the State prosecutor at the district court of Luxembourg.
As far as the other professionals of the financial sector are concerned, this person shall be a manager in possession of the legally required authorisation and who has been specifically appointed to this function.

III. Risk-based approach

4. In the context of the fight against money laundering and terrorist financing, the professionals of the financial sector shall adopt an approach focused on the real risk, both during the customer identification process and the monitoring of transactions, while taking into account the particularities of their respective activities and their differences in scale and size.

5. As the Luxembourg framework on the fight against money laundering and terrorist financing, in the light of the existing regulations at European and global level, consists of a criminal and a preventive part, Part I of this Circular deals with the money-laundering and terrorist-financing offences and Part II with the professional obligations.

Part I Money-laundering and terrorist-financing offences

6. Luxembourg law provides for specific money-laundering and terrorist-financing criminal offences.
Article 1 of the law of 12 November 2004 on the fight against money laundering and terrorist financing as amended provides that:

- "Money laundering" shall mean any action as defined in Articles 506-1 of the Penal Code and 8-1 of the amended law of 19 February 1973 concerning the sale of medicinal substances and measures to combat drug addiction;
- "Terrorist financing" shall mean any action as defined in Article 135-5 of the Penal Code.

Title 1 The money-laundering offence

7. In accordance with Articles 506-1 and 8-1 above, the money-laundering offence is defined as follows:

- "knowingly facilitating by any means the false justification of the source of the property constituting the object or the direct or indirect proceeds, or constituting a patrimonial benefit of any nature whatsoever from one or several of the designated predicate offences;

- knowingly assisting in a placement, dissimulation or conversion transaction of property constituting the object or the direct or indirect proceeds, or constituting a patrimonial benefit of any nature whatsoever from one or several of the predicate offences;

- having acquired, held or used the property constituting the object or the direct or indirect proceeds, or a patrimonial benefit of any nature whatsoever from one or several of the predicate offences, knowing, at the time they received them, that they originated from one of the designated offences or from the participation in one or several of these offences".

These Articles define the money-laundering offence while listing the facts constituting this offence and specifying the categories of predicate offences which may give rise to this offence.

Chapter 1 Predicate offences

8. Money laundering presupposes the existence of a predicate offence whose object or proceeds may give rise to a money-laundering offence.

The predicate offences include those listed below. They have been classified according to the list of designated categories of offences included in the glossary of the 40 FATF recommendations. The enumeration however cannot be exhaustive given that the list in

question refers not only to those offences explicitly laid down in Article 506-1 of the Penal Code and in Article 8-1 of the law of 19 February 1973 concerning the sale of medicinal substances and measures to combat drug addiction but also to other offences which, in accordance with the last subparagraph of the same Article 506-1, are punishable "by imprisonment of more than 6 months":

Involvement with an organised criminal gang and a racket:

- the crimes and offences perpetrated within the scope or in relation with an association created with the purpose of attempting on persons or properties or within the scope or in relation with a criminal organisation) (Articles 322 or 324ter of the Penal Code);

Terrorism, including financing thereof:

- offences of terrorism and terrorist financing (Articles 135-1 to 135-6 of the Penal Code);

Human trafficking and illicit trafficking of immigrants:

- sexual offences on minors (Article 379 of the Penal Code)
- procuring (Article 379 bis of the Penal Code);
- offences listed in Article 33 of the law of 28 March 1972 as amended relating to: 1. the entry and stay of foreigners; 2. the medical control of foreigners; 3. the hiring of foreign workers as laid down in Article 143 of the law of 29 August 2008 concerning the free movement of persons and immigration;

Sexual exploitation, including of minors:

- offences listed in Articles 372 to 377 of the Penal Code;
- sexual offences on minors (Article 379 of the Penal Code)
- procuring (Article 379 bis of the Penal Code);

Illicit trafficking in narcotic drugs and psychotropic substances:

- offences listed in Article 8-1 of the law of 19 February 1973 concerning the sale of medicinal substances and the fight against drug addiction;

Arms trafficking:

- offences listed in the legislation on arms and ammunition (notably the law of 15 March 1983 on arms and ammunition);

Illicit trafficking in stolen goods and other goods:

- offences listed in Article 10 of the law of 21 March 1966 concerning a) historic, pre-historic, paleontological or otherwise scientific excavations; b) the safekeeping of moveable cultural heritage;
- offences listed in Article 5 of the law of 11 January 1989 on the commercialisation of chemical substances for therapeutic purposes;
- offences listed in Article 18 of the law of 25 November 1982 on the sampling of substances of human origin;

Corruption:

- public and private corruption (Articles 246 to 253, 310 and 310-1 of the Penal Code)

Fraud and swindle:

- offences listed in Articles 489 to 490 of the Penal Code (bankruptcy);
- offences listed in Articles 491 to 495 of the Penal Code (breach of trust);
- offences listed in Article 496 of the Penal Code (swindle);
- frauds against the financial interests of the State and international institutions (Articles 496-1 to 496-4 of the Penal Code);

Forgery of money:

- offences listed in Articles 162 to 178 of the Penal Code (in the cases where the minimum imprisonment is of more than 6 months) [1] ;

Forgery and product piracy;

- offences listed in Articles 184, 187, 187-1, 191 and 309 of the Penal Code;
- offences listed in Articles 82 to 85 of the law of 18 April 2001 on copyright;

Crimes and misdemeanours against the environment:

- offences listed in Article 64 of the law of 19 January 2004 as amended concerning the protection of nature and of natural resources;
- offences listed in Article 9 of the law of 21 June 1976 as amended concerning the flight against pollution of the environment;
- offences listed in Article 25 of the law of 10 June 1999 as amended concerning classified buildings;
- offences listed in Article 26 of the law of 29 July 1993 concerning water protection and management;
- offences listed in Article 35 of the law of 17 June 1994 as amended concerning the prevention and management of waste;

Murder and bodily harm (*coups et blessures*):

- offences listed in Articles 392 to 410 of the Penal Code (in the cases where the minimum imprisonment is of more than 6 months) [1];

Kidnapping, illegal detention and taking of hostages:

- offences listed in Articles 368 to 370 of the Penal Code (abduction of minors);
- offences listed in Article 442 of the Penal Code (taking of hostages)[1];

Theft:

- offences listed in Articles 463 to 464 of the Penal Code;

[1] pursuant to the last sub-paragraph of Article 506-1 of the Penal Code

- offences listed in Articles 467 to 479 of the Penal Code (aggravated theft, theft with violence or threats) (in the cases where the minimum imprisonment is of more than 6 months) [1] ;

Smuggling:
- offences listed in Articles 220 to 231 of the general law on customs and excise (douanes et accises);

Extortion:
- offences listed in Article 470 of the Penal Code[1] ;

Forgery:
- offences listed in Articles 193 to 212 of the Penal Code (in the cases where the minimum imprisonment is of more than 6 months) [1];

Piracy:
- offences listed in Article 31 of the law of 31 January 1948 as amended concerning aerial navigation[1] ;
- offences listed in Article 64 of the disciplinary and penal code for the marine[1];

Insider dealing and market manipulation:
- offences listed in Article 32 of the law of 9 May 2006 on market abuse.

It should be stressed that a money-laundering offence has been committed even where the predicate offence has been committed abroad, provided however that such offence constitutes a predicate offence both in Luxembourg and abroad.

Chapter 2 Material element

9. Money laundering consists of any act relating to the proceeds or the object i.e. to any economic benefit drawn from the predicate offence.

The legal definition of money laundering is very broad and encompasses a whole set of devices which all serve the purpose to provide a false justification of the origin of the property forming the object or proceeds of the predicate offences.

Chapter 3 Intentional element

10. For the money-laundering offence to be given, the intentional element is the determining factor. Whoever knowingly launders the proceeds or the object originating from the predicate offences commits a money-laundering offence.

Title 2 Terrorist-financing offence

11. Pursuant to Article 135-5 of the Penal Code, the offence of terrorist financing is defined as "providing or collecting by any means, directly or indirectly, unlawfully and intentionally, funds, assets or properties of any nature, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences referred to in Articles 135-1 to 135-4 and 442-1[2], even if they have not actually been used to commit one of these offences."

Title 3 Criminal offences

12. Whoever commits a money-laundering offence is punishable by sanctions of imprisonment (1 to 5 years) and/or fines (1,250 to 1,250,000 Euros) under Articles 506-1 and 8-1 mentioned above.
It should be borne in mind that the perpetrator, the co-perpetrators and the accomplices are punishable under the terms of these Articles.
Whoever commits a terrorist financing offence is punishable under Articles 135-1 to 135-4 and 442-1 of the Penal Code according to the distinctions established therein.
It should be stressed at this point that the violation of the professional obligations as referred to in items 13 to 144 of this Circular is also penally sanctioned as laid down in point 153 below.

[2] Article 442 of the Penal Code deals with the taking of hostages.

Part II Preventive part of the anti-money laundering and anti-terrorist financing framework: professional obligations

Title 1 Scope of application of the professional obligations

Chapter 1 Material scope of application

13. The law of 12 November 2004 as amended extended the professional obligations on the fight against money laundering to the fight against terrorist financing, an offence defined in Article 135-5 of the Penal Code. As a consequence, the preventive means to combat money laundering and terrorist financing are of the same nature.

Chapter 2 Personal scope of application

Section 1 Professionals of the financial sector exercising in Luxembourg

14. The group of persons submitted to the professional obligations has been extended by the law of 12 November 2004 as amended to other players of the financial sector, as well as to other defined persons not belonging to this particular sector, but to whom the fight against money laundering and terrorist financing is particularly relevant.

15. This Circular applies exclusively to the professionals of the financial sector subject to the professional obligations that fall under the supervision of the CSSF. They shall hereafter be referred to indifferently as "professionals" or "professionals of the financial sector".

They are the following:

- credit institutions and other professionals of the financial sector (PFS) licensed or authorised to carry on their activities in Luxembourg in accordance with the law of 5 April 1993 on the financial sector as amended.
  These include not only to the credit institutions licensed as universal banks, but also to institutions with special statuses such as electronic money institutions;

- other professionals of the financial sector (PFS): not only all PFS specifically listed under Part I, Chapter 2 (Articles 24 to 29-5) of the law of 5 April 1993 on the financial sector as amended**,** but also all other persons carrying on financial sector activities and licensed thereto in accordance with Article 13(1) of said law;

- undertakings for collective investment and investment companies in risk capital (SICAR), which market their units or shares and to which the law of 20 December 2002 relating to undertakings for collective investments, as amended, or the law 13 February

2007 on specialised investment funds or the law of 15 June 2004 relating to the investment company in risk capital (SICAR) applies.

The law of 12 November 2004 as amended imposes the identification requirements on those UCIs that market their units themselves i.e. that are in direct contact with the investors, as they market their units without having recourse to other professionals. It should be stressed that the UCIs that market their units themselves may rely on third parties for the material execution of the identification requirements under the terms described in points 95 to 104 below.

The subscriptions and repurchases in UCIs that do not market their units themselves are necessarily done via intermediaries. Such UCIs shall not be subject by law to the due diligence requirements insofar as the intermediary is a credit or financial institution (as defined in Article 2(2) of the law of 12 November 2004 as amended) which is subject to equivalent requirements to those laid down in the law of 12 November 2004 as amended.

Where the intermediary is not a credit or financial institution subject to equivalent requirements to those laid down in the law of 12 November 2004 as amended, the responsibility for the identification of the intermediary and of the investors (as beneficial owners) lies with the relevant UCI/the Luxembourg professional.

- management companies under the law of 20 December 2002 relating to undertakings for collective investment as amended which market units/shares of UCIs or perform additional or auxiliary activities within the meaning of the law of 20 December 2002 as amended relating to undertakings for collective investment;

- pension funds under the prudential supervision of the CSSF, i.e. assep and sepcav governed by the law of 13 July 2005 as amended.

16. As the provisions of the law of 12 November 2004 as amended are deemed to be of public order, they must be complied with by the professionals of the financial sector conducting their business in Luxembourg in the form of a subsidiary (Article 2(2) of the law of 12 November 2004 as amended) or a branch.

Professionals operating in Luxembourg under the freedom to provide services from an institution based abroad shall adopt the provisions concerning the fight against money laundering and financing of terrorism of their home country, provided that they are subject in such country to regulation concerning the fight against money laundering and terrorist financing which is equivalent to the Luxemburg regulation. If this is not the case they shall respect the applicable Luxembourg regulations.

Conversely, Luxembourg professionals operating abroad under the freedom to provide services shall apply the Luxembourg provisions concerning the fight against money laundering and financing of terrorism.

Section 2 Branches and subsidiaries abroad of the concerned professionals of the financial sector conducting business in Luxembourg (Article 2))

Sub-section 1 General principle

17. The branches and subsidiaries (of those professionals covered by this Circular) established in another Member State of the European Union or of the European Economic Area are subject in the respective host State to the regulation of such host State concerning the fight against money laundering and terrorist financing equivalent to the Luxembourg or European regulations.

18. As regards branches and subsidiaries established in third countries i.e. countries which are neither members of the European Union nor of the European Economic Area, Article 2(2) of the law of 12 November 2004 as amended sets out that among the professionals covered by this law, credit and financial institutions (as defined in Article 2(2) of the law of 12 November 2004 as amended) shall apply in their branches and majority-owned subsidiaries measures at least equivalent to those laid down in the law of 12 November 2004 as amended or Directive 2005/60/CE as regards customer due diligence and record keeping.

To this end, credit and financial institutions (as defined in Article 2(2) of the law of 12 November 2004 as amended) shall communicate the relevant policies and procedures, where applicable, to branches and majority-owned subsidiaries located in third countries.

As regards companies in which the professional of the financial sector holds a stake which is not a majority holding but lies between 20% and 50%, it is the professional of the financial sector that is not the parent company, to do its utmost, together with the other shareholders or partners concerned, to see that a system of anti-money laundering and terrorist financing which meets the same standards as those in force in Luxembourg is set up.

Sub-section 2 Branches and subsidiaries established in a third country for which the regulation does not allow to apply equivalent measures

19. Where the institution in question (as referred in point 18 above) notes that provisions exist in the third country which prevent them from applying measures which are at least equivalent to Luxembourg or European standards as regards customer due diligence and record keeping, the relevant credit and financial institutions have to notify the CSSF so that the problem can be raised with the European Commission in accordance with Article 31(2) of Directive 2005/60/EC.

The obligation to notify the CSSF exists for all third countries as defined in Article 1(5) of the law of 12 November 2004 as amended, including those listed in Grand-ducal regulation of 29 July 2008 establishing the list of "third countries which impose equivalent requirements".

The credit and financial institutions in question shall also take additional steps in order to efficiently face up to the risk of money laundering or terrorist financing which may result

from the situation/deficiencies of the regulation in question. They shall inform the CSSF of measures actually taken in this context.

It should be stressed that non-compliance with the professional obligations imposed on branches and subsidiaries by Luxembourg law, or with those of the foreign law if it is more stringent, may jeopardise the authorisation required for operating such branches and subsidiaries or even the authorisation to conduct business in the Luxembourg financial sector.

Sub-section 3 Controlling compliance with the professional obligations in subsidiaries and branches

20. The anti-money laundering and terrorist financing officer is responsible for checking compliance with the professional obligations in branches and subsidiaries referred to in point 18.

In addition, internal audit and the anti-money laundering and terrorist financing officer of the parent company or the head office are required to verify periodically, in accordance with point 152 below, that the branches and subsidiaries referred to in points 18 and 19 respectively, actually comply with all their professional obligations so that they shall at least be in compliance with the law of 12 November 2004 as amended or Directive 2005/60/CE in accordance with Article 2(2) of said law.

Concerning the companies referred to in the third paragraph of point 18, the professional of the financial sector shall endeavour to obtain a summary of the audit and/or compliance reports of these companies and shall have them analysed by the anti-money laundering and terrorist financing officer.

Title 2 Content of the professional obligations

21. In accordance with the law of 12 November 2004 as amended, the following anti-money laundering and terrorist financing professional obligations apply to the professionals of the financial sector:

1. obligation to perform customer due diligence (Article 3 (2));
2. obligation to pay special attention to certain activities and transactions (Article 3(7))
3. obligation to keep certain records and information (Article 3(6));
4. adequate internal management requirements (Article 4);
5. obligation to co-operate with the authorities and obligation to report (Article 5).

An additional specific professional obligation is imposed only on credit institutions and other professionals of the financial sector (PFS), namely:

6. obligation to include on wire and funds transfers as well as on associated messages information on the payer in accordance with Regulation 1781/2006 of the European Parliament and the Council of 15 November 2006 relating to the information on the payer accompanying transfers of funds as regards wire transfers.

22. In order to ensure a proper and consistent implementation of these professional obligations, all professionals of the financial sector shall comply with the detailed instructions set out below.

Chapter 1 Customer due diligence

Section 1 Customer due diligence procedures

23. In accordance with Article 3(1) of the law of 12 November 2004 as amended, professionals shall perform customer due diligence in the following situations:

a) when establishing a business relationship;

b) when carrying out occasional transactions amounting to EUR 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

In accordance with Article 3(2) of the law of 12 November 2004 as amended, the customer due diligence procedures shall include:

a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

b) identification of the beneficial owner(s), where this is not the customer, and taking risk-based and adequate measures to verify their identity or to understand the ownership and control structure of the legal person, trust or similar legal arrangements.

   Identification must thus go further than the direct customer and extend to the persons on whose behalf the direct customer is acting, commonly referred to as "beneficial owner".

c) obtaining information on the purpose and intended nature of the business relationship;

d) conducting ongoing monitoring of the business relationship and keeping up-to-date the documents, data or information held.

Article 3-2(5) of the law of 12 November 2004 as amended, contains a prohibition to open an account which is directed at any correspondent banking relationship with a shell bank or with a bank that is known to permit its accounts to be used by a shell bank (see point 89 below).

24. Risk-based approach: Professionals shall implement each of the customer due diligence measures set out in Article 3(2) of the law of 12 November 2004 as amended, but they may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. Professionals shall be able to demonstrate that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing. The professional shall include the justification for the adaptation of customer due diligence measures on a risk-sensitive basis in the internal procedures as set out in Article 4(1) of the law of 12 November 2004 as amended.

The risk-based approach only allows professionals of the financial sector to establish and adapt the scale of the customer due diligence on a risk-sensitive basis to the customer or the transaction but it does not allow professionals to simply waive one, several or all of the measures.

When professionals of the financial sector are faced with situations which present a high risk of money laundering or terrorist financing, whether in the specific cases set out in Article 3-2 of the law of 12 November 2004 as amended or in those considered as such by a professional following his risk-assessment, the measures laid down in Article 3 of the law of 12 November 2004 as amended are no longer sufficient. In this case, professionals shall take enhanced customer due diligence measures as laid down in Article 3-2 of the law of 12 November 2004 as amended and as set out in points 80 to 94 of this Circular. There are also situations where the risk of money laundering or terrorist financing is considered to be low: in such case, Article 3-1 of the law of 12 November 2004 as amended, allows the application of simplified customer due diligence in a limited number of specific cases (points 105 to 111 of this Circular).

Sub-section 1 Identification of customers and verification of their identity

25. The law distinguishes between ongoing relationship customers and occasional customers.

A. Customers in a business relationship

Paragraph 1 Concepts of business relationship and of customer

26. Professionals shall perform customer due diligence as set out in Article 3(1) of the law of 12 November 2004 as amended when they enter into a business relationship with a customer, i.e. in accordance with the law of 12 November 2004 as amended, a business, professional or commercial relationship which is connected with the professional activities of the professionals and which is expected, at the time when the contact is established, to have an element of duration.
The notion of "customer" does not only encompass the person on whose behalf an account or savings account is opened, but also all co-account-holders and proxies.

27. Each professional of the financial sector must require identification of their customers by means one or more documents, data or information obtained from a reliable and independent source when entering into a business relationship, in particular, when opening an account or a savings account, or when offering safe custody facilities, be it in the form of account opening or safe custody services.
As setting up a business relationship entails in principle, in one form or another, the "opening of an account", this expression will be hereafter used in this sense.

28. Ongoing customers shall also include those customers who open payable-through accounts solely for the purpose of one or more one-off transactions.

Paragraph 2 Preliminary nature of the identification and verification of the identity

a. General principle

29. In accordance with Article 3(4) of the law of 12 November 2004 as amended, the identification of the customer and of the beneficial owner as well as the verification of their identities shall take place before the establishment of a business relationship or opening of an account or the carrying-out of the transaction respectively. This means that in principle the identification and verification of the customer's identity shall take place from the moment of the initial contact.

As the verification of the identity may be more time-consuming, it is possible that this be done during the establishment of the business relationship i.e. that it be slightly removed in time in comparison to the identification of the customer. This procedure is accepted so as to not interrupt the normal conduct of activities provided the resulting risk of money laundering or terrorist financing is only low according to the professional's assessment. During this time, while the verification of the identity is taking place, it is not permitted to open an account nor to execute a transaction for the customer.

On the other hand, in these circumstances it is only permitted to open an account on the terms described in point 30 below.

30. As a matter of fact, by way of derogation to the rules described above, the fourth sub-paragraph of Article 3(4) nevertheless allows the opening of a bank account without verification of the customer's identity, provided that no transaction be executed by the customer or on his/her behalf until the verification of the identity be complete to the professional's satisfaction. To this end, sufficient safeguards need to be in place to ensure that no transaction is executed in these circumstances: the safeguards have to be integrated within the credit institution's internal procedures.

Regarding the transaction, it must be stressed that a transfer crediting the bank account is not contemplated, but only those operations disposing of assets through the customer's bank account.

If the professional of the financial sector accepts to receive funds from a customer on an account opened in accordance with the terms set out in the fourth sub-paragraph of Article 3(4), before completion of the verification of the customer identification or as the case may be, of the beneficial owner, or, on a temporary basis and on a frozen account, the professional of the financial sector may not return the funds, through cash payments or transfer, for the benefit or on the orders of this customer, as long as the customer’s identity has not been fully established. In the meantime, the professional of the financial sector shall continue to ensure the custody of the assets in the customer’s interest, in accordance with the terms agreed upon at the time of the deposit, unless the professional pays them into court if all the conditions therefore are fulfilled.
If professional note that they are unable to comply with the customer due diligence measures set out in Article 3(2)(a) to (c) of the law of 12 November 2004 as amended, they must not

carry out a transaction through a bank account, establish a business relationship nor carry out a transaction. If a business relationship exists it shall be terminated. In all these cases, professionals shall consider making a suspicious transaction report to the State prosecutor at the district court of Luxembourg.

It must be stressed that professionals of the financial sector shall be held liable should they allow customers to have access to the funds or to simply state the account's existence before full completion of the identification and verification of the customer's identity.

In accordance with the fourth sub-paragraph of Article 3(4) of the law of 12 November 2004 as amended, the opening/keeping of anonymous accounts or anonymous savings account is prohibited. This prohibition stems from the obligation to identify and to know the customer on the basis of the customer due diligence measures referred in point 23 above. The professionals shall apply appropriate measures so that the prohibition of the opening/keeping of such accounts or savings accounts is followed. Where numbered accounts or savings accounts are opened, professionals shall manage the accounts at all times in full compliance with the obligations they are subject to in accordance with the law of 12 November 2004 as amended and with this Circular.

Customers introduced by third parties

31. An account opening may be requested for a customer by a professional of the financial sector with whom the customer already has an account and who is acting as a third party in the performance of customer due diligence as referred to in Article 3-3 of the law of 12 November 2004 as amended and in points 95-104 of this Circular. In this case the account may be opened under the responsibility of the professional to whom the client is being introduced, based on the receipt of the mandatory information, without need for a new identification or verification of the identity of the customer.

b. Exception

Companies in the process of incorporation

32. It is allowed to open an account for a company in the process of incorporation, subject to the identification and verification of the identity of the company's founders and to deliver to a notary a certificate of escrow for the funds held in the account. The identification and verification of the identity of the founders shall be accompanied by a declaration of the founders stating that they act either on their own behalf or on that of the appointed beneficial owners. The identification and verification of the identity of the company has to be completed as soon as possible on hand of the documents listed in point 40 below (Articles of incorporation, recent extract from the trade register or equivalent documents) and before the release of any funds by the professional of the financial sector concerned. The same also applies to the identification and verification of the identity of the beneficial owners of the company appointed by the founders and any other beneficial owners for whom the identification and verification of the identity has to be completed in accordance with point 47 and following of this Circular.

c. Mandatory written authorisation

33. The opening of an account for a new customer shall be submitted for approval in writing to an officer or a body of the professional of the financial sector duly empowered for this purpose. This officer or body shall assess both whether an account should be opened for this customer and assume responsibility for the identification and the verification of the identity of the customer and, if appropriate, the beneficial owner and the related documentation.

34. As regards the customers considered as bearing a high risk, including those referred to in points 80-94 below, enhanced due diligence measures are mandatory.

Paragraph 3 Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source

35. Article 3(2)(a) of the law of 12 November 2004 as amended establishes the obligation to identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source. Whereas in the past the operation of verification was inherent to the notion of "customer identification", the new Article 3(2)(a) distinguishes between identification and verification.

Thus, the act of identification consists of bringing a customer out of anonymity and giving him/her a name, an identity. Identification can be done for instance by completing an application form to enter into business relations and to indicate thereon the number of an identity document. The act of verification on the other hand consists of establishing a link with reality by ensuring that this identity in fact relates to the person one is dealing with, that this person exists in reality and that the documents, data or information are both trustworthy and conclusive. They may be made available by the customer, although the obligation that they be independent means they cannot be produced by the customer himself.

Generally the identification of natural persons as well as legal entities and the verification of their identity are done in one single step on the basis of official documents.

A distinction should be made between customers who are natural persons and those who are legal persons.

a. Natural persons

36. The identification and verification of the natural-person customer shall be made in principle on the basis of an official identification paper which certifies the identity of the person (e.g. passport, identity card, driving license, residence permit, or any other official document carrying a photograph allowing to unequivocally identify the person concerned).

If the customer does not hold identification documents which correspond exactly to the required criteria, professionals of the financial section shall verify the identity of the customer based on documents from different sources while completing the necessary verification in order to ascertain the customer's identity with a sufficient degree of certainty. If the identity of the customer cannot be verified with sufficient certainty the professional shall refuse to enter into a business relation and to carry out any transaction. If there is a suspicion of money laundering or financing of terrorism, the professional shall make a report to the State prosecutor at the district court of Luxembourg. (see points 118 and following of this Circular).

37. The professionals of the financial sector shall also:

- ensure that the documents produced really belong to their holder by comparing the signature on the identification document to that on the account opening form and, where applicable, by comparing the photograph on the identification document with the customer in person;

- on a risk-sensitive basis, make a copy of the identity documents and keep them on file, or transcribe the following information on the account opening form: surname and first name, date and place of birth, nationality, full address, profession, number of the identity card;

- ensure that the account opening request is signed by the customer on a form of the Luxembourg professional of the financial sector;

- ensure that all the account opening documents are duly and legibly completed, dated and signed by the customer.

38. Where the customer carries on a financial activity that involves the management of third-party funds, a copy of the relevant authorisation or a note that such authorisation is not required, shall be placed on file.

b) Legal persons:

39. Formal identification and verification must be made at two levels, namely:

- legal person;
- representatives (proxies) of the legal person.

I. Identification and verification of the identity of the legal person

40. Identification and verification of a legal-entity customer must be based on the following documents:

1) Articles of incorporation (or equivalent)
2) recent extract from the trade register (or equivalent).

As far as documents 1) and 2) above are concerned, the purpose is to obtain proof of the incorporation and of the legal status of the legal person (nationality, legal form), as well as information on the name of the company, the name of the directors and managers and the provisions governing the power to commit the entity, as well as the address of its registered office.

As far as the latter point concerned, the professionals are required to enquire whether the company is domiciled in Luxembourg and, if so, with whom. Where the entity is a foreign company with an address in Luxembourg, the professionals of the financial sector shall in addition obtain clear and precise information on the jurisdiction in which the company is incorporated or organised, and, where applicable, the address of its principal place of business abroad. These items of information may be obtained from public registers, the customer or other reliable sources.

41. Where the customer carries out a financial activity that involves the management of third-party funds, a copy of the relevant authorisation or a note that such authorisation is not required, shall be placed on file.

II. Identification and verification of the identity representatives (proxies) of the legal person

42. Identification and verification of the representatives (proxies) of the legal persons or the persons empowered by these bodies is, in principle, limited to those persons who are members of the bodies of the legal person acting on behalf of the company in its relation with the professional of the financial sector, i.e. those empowered to operate the accounts of the legal person with the professional of the financial sector. The identification and verification of the identity of such persons shall be identical to that for natural-person customers.
The professional of the financial sector must also verify whether the competent governance body has effectively authorised the account opening concerned and whether the persons empowered to operate the account are effectively entitled thereto under the terms of the Articles of incorporation or a resolution of the competent governance body.

c. Verification in situations which require the application of enhanced due diligence

43. While conducting the identification and verification of the identity, the professional of the financial sector has to verify whether the customer in question warrants the application of enhanced due diligence in accordance with Article 3-2 of the law of 12 November 2004 and points 80 to 94 of this Circular. The professional shall verify in particular if the customer, the beneficial owner(s) and the persons empowered to operate the account do not appear on the list of terrorists circulated via the circulars listed in Annexe III to this Circular.

B. Occasional customers

44. The identification and verification of the identity and the application of further due diligence measures also applies where transactions, executed for customers other than those with whom a business relationship has been established, amount to EUR 15,000 or more, whether they are carried out in a single operation or in several operations which appear to be linked. Where the total amount of the transaction is unknown when the parties commit to the transaction, the professional of the financial sector shall perform the identification and verification of the identity as soon as the amount is known and the EUR 15,000 threshold reached. The professionals of the financial sector are required to identify and to verify the customer's identity even if the total amount of the transaction is below the EUR 15,000 threshold if there is any suspicion of money laundering or terrorist financing.
This requirement applies to occasional transactions, notably at the bank counter, for which no file is prepared or account opened.

45. Where identification and verification of an occasional customer is required, they shall be carried out and documented in accordance with the same procedures as those applying to customers engaged in a business relationship.
The situation in which identification and verification of the identity of an occasional customer becomes mandatory due to suspicions of money laundering or terrorist financing, calls on the judgement of the professional of the financial sector.
Where identification of such customer, and, where applicable, his answers to the professional's additional questions are insufficient to remove, or conversely confirm the suspicion, the professional of the financial sector shall refrain from executing the transaction and file a suspicious transaction report with the State prosecutor (see points 118 and following of this Circular).

46. It should be borne in mind that specific laws, adopted for purposes other than for anti-money laundering, impose identification requirements over and above those laid down in the law of 12 November 2004 as amended. Compliance with these specific laws is of course mandatory, notably with Article 5 of the law of 3 September 1996 as amended concerning the involuntary dispossession of bearer shares, which requires that all professionals of the financial sector verify and record the exact identity of the persons with whom they carry out share operations, regardless of the amount involved. The same applies to Article 74 of the law of 9 November 1797 on the monitoring of gold and silver, which requires professionals

of the financial sector to record the identity of the persons to whom or from whom they sell or buy gold or silver.

Sub-section 2 Identification and verification of the identity of beneficial owners

Paragraph 1 Definition of the beneficial owner

47. Article 1(7) of the Law of 12 November 2004 as amended defines the beneficial owner as any natural person who ultimately owns or controls the customer and/or any natural person on whose behalf a transaction or activity is being conducted.

The beneficial owner shall at least include:

(a) in the case of corporate entities:

i) any natural person who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards; a percentage of more than 25% shall be deemed sufficient to meet this criterion;
ii) any natural person who otherwise exercises control over the management of a legal entity:

b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:

i) where the future beneficiaries have already been determined, any natural person who is the beneficiary of 25% or more of the property of a legal arrangement or entity;
ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
iii) any natural person who exercises control over 25% or more of the property of a legal arrangement or entity.

48. It should be borne in mind that "beneficial owners" are also referred to as “persons on whose behalf the customer is acting" , "economic owners" or "beneficiaries" (*bénéficiaires réels ou ayants droit économiques*).

Paragraph 2 General rules

49. Article 3(2)(b) of the law of 12 November 2004 as amended obliges professionals to identify the beneficial owner if the customer is not acting on his own account. The professional therefore has to gather information regarding the identity of the beneficial

owner. This obligation equally applies whether the customer is a natural person, a legal person, a trust or a legal arrangement.
As regards the verification of the identity of the beneficial owner the law does not require that it be based on information obtained from a reliable source, as is the case for the verification of the customer's identity, but it adopts a more flexible approach based on risk.
Thus professionals have to take adequate and risk-based measures to verify the identity of the beneficial owner so that they are satisfied they know who the beneficial owner is.
As regards customers that are legal persons, trusts or legal arrangements, the adequate measures to be taken by professionals, the importance of which also depends on the risk of money laundering and terrorist financing, are aimed at allowing them to understand the ownership structure and control of the customer.
In this context WHEREAS 10 of Directive 2005/60/CEC is of use, which states that to fulfil this requirement it should be left to professionals whether they make use of public records of beneficial owners, to ask their customers for relevant data or to obtain the information otherwise, taking into account the fact that the extent of such customer due diligence measure relates to the risk of money laundering and terrorist financing, which depends on the type of customer, business relationship, product or transaction.

50. Identification/verification of the identity of the beneficial owner is a key element of information as regards customer identification allowing to better know the customer. Suspicions of money laundering or terrorist financing associated with the beneficial owner thus reflect on the customer and must be reported to the State prosecutor in accordance with Article 5(1) of the law of 12 November 2004 as amended and points 118 and following of this Circular.

51. Nevertheless, in a situation where simplified due diligence as laid down in Article 3-1 of the law may be applied, the identification of any beneficial owners is not required.

Paragraph 3 Natural persons

52. In general, during the identification process, it is recommended that professionals of the financial sector require a written declaration stating that the customer is acting for his/her own account or, as the case may be, that he/she is not the beneficial owner/does not act for his/her own account . As regards a natural-person customer, it is primarily the first part of the definition above which is relevant. It is the natural person who ultimately controls the customer and/or any natural person for whom a transaction or activity is being realised.

Where the professional of the financial sector is certain that the customer is not acting for his/her own account, notably by virtue of his/her declaration, the professional shall obtain the relevant information from the customer relating to the identity of the beneficial owner(s). As regards verification of this information, the professional has to take adequate measures based on the risk of money laundering and terrorist financing and in particular has to get the necessary documents from the customer to establish the identity of the beneficial owner(s). It is recommended that the professional of the financial sector always requires a written declaration from the beneficial owners themselves in confirmation of the customer's statements.

53. Where professionals of the financial sector have a doubt as to whether the customer is acting on his/her own account, professional should dispel the doubt either by obtaining a written and credible confirmation from the customer that the latter is acting on his/her own account, or by identifying the beneficial owner in the manner described above. It must be stressed that the doubt is not necessarily removed by a negative statement from the customer or by the fact that a third party confirms being the beneficial owner. Where professional of the financial sector are not able to remove the doubt, they shall refrain from dealing with the customer.
Furthermore, they shall, where applicable, consider filing a report with the State prosecutor.

Special case: Customers whose professional activities imply the holding of third-party funds (i.e. lawyers, notaries, etc)

54. Where a notary or a member of another independent legal profession (for instance a lawyer) wishes to open an account with a professional of the financial sector, the latter shall expressly ask such customers whether they are acting on their own behalf or on behalf of others and shall assess the plausibility of the response so as to determine whether the opening of a pooled account is necessary. Professional of the financial sector shall obtain from the customer, at the time of the acceptance process and during the ongoing business relationship, the information they deem necessary to make sure that the relations are not being used for money-laundering or terrorist financing purposes.
Where such customers are acting on their own behalf, the usual identification procedures set out in this Circular apply.

55. Where such customer is acting on behalf of third parties, it is worth reiterating that the persons referred to above may open accounts serving basically two different purposes:

(a) The funds passing through these accounts may be connected with the professional activity of the above persons consisting in assisting their clients in the planning and execution of transactions regarding in particular:

- buying and selling of real property or business entities;
- management of money, securities or other assets belonging to the customer;
- organisation of contributions necessary for the creation, operation or management of companies or similar structures;
- creation, domiciliation, operation or management of trusts (fiducies, fondations), companies or other similar structures.

In the circumstances mentioned above, in accordance with Article 3-1(2)(b) (and as also mentioned in point 110 of this Circular), the professional acting as depositary of funds can apply simplified customer due diligence measures, i.e. the professional acting as depositary may open a pooled account without having to identify the beneficial owners. However, this is only possible if the customer is a notary or a member of another independent legal profession (for instance a lawyer) from a Member State or a third country in which such professions are subject to requirements to combat money

laundering and terrorist financing consistent with international standards (cf. list of "third countries which impose equivalent requirements" published by way of Grand-ducal regulation of 29 July 2008) and where compliance with such requirements is supervised. It should furthermore be stressed that, pursuant to Article 3-1(2)(b) of the law of 12 November 2004 as amended, information regarding the identity of the beneficial owners has to be submitted to the relevant professional acting as depositary on request.

Before opening a pooled account without identification of the beneficial owners, professionals acting as depositary must ensure that the customer in question fulfils the conditions above and, where appropriate, they shall request a written undertaking from the customer that they shall on request immediately submit information regarding the identity of the beneficial owners. It is recommended to also request a certificate from the relevant professional association that there is no professional obligation which would prevent the notary or the member of the independent legal profession in question to make such information available to the professional acting as depositary (see also point 11 of this Circular).

If the customer does not fulfil the conditions above, the identification of the beneficial owners has to be completed before the pooled account is opened.

(b) The funds passing through these accounts are related to any other professional activity of the aforementioned persons, consisting in particular in advising their customers as regards the assessment of the legal situation of the latter, excluding the activities referred to under point (a) above or in representing the customer in legal proceedings.
In this case, the professional of the financial sector shall assess the plausibility of the statements of these persons and may refrain from identifying the beneficial owners if the professional is satisfied by the explanations given by these persons.

56. In all cases, the professionals of the financial sector are under the ongoing obligation to carefully monitor the transactions carried out by these persons and must gather all the information necessary to remove any risk of money laundering or terrorist financing.

Paragraph 4 Legal persons

57. Where a professional of the financial sector wishes to enter into a business relationship with a legal person, trust or similar legal arrangement, the person(s) that have to be identified in their capacity as beneficial owners must always be natural persons. In accordance with the law, reference is made to any natural person who ultimately owns or controls the customer and/or any natural person on whose behalf a transaction or activity is being conducted. The law of 12 November 2004 as amended, in its definition of beneficial owner (point 47 above) provides precise explanations as to the nature and importance of the relationship which a natural person must have with a legal person, a trust or legal arrangement in order to qualify as a beneficial owner.

It should be borne in mind that, contrary to the verification of the identity of the beneficial owner, the identification is in itself a measure of due diligence which cannot be adapted according to the risk of money laundering or terrorist financing given that it simply consists of making available the name, place and date of birth, nationality and residential address of a natural person. To this end the professional of the financial sector will mainly rely on the information provided by the customer.

58. The verification of the identity of the beneficial owner(s) of a legal person, a legal arrangement or a trust includes understanding the ownership and control structure of the customer.
In order to fulfil this duty in a satisfactory manner, the professional of the financial sector shall adopt a risk-based approach.

Pertinent items of information or data on the beneficial owners and on the control of legal persons may be obtained from public registers or from other reliable and independent sources.

59. The professional of the financial sector shall request a written and credible declaration from a person who fulfils the criteria of the definition of beneficial owner described in point 47, certifying that he/she is the beneficial owner. If the professional cannot obtain such a declaration or if the professional has doubts regarding the veracity of the declaration by a person who affirms to be the beneficial owner and this doubt cannot be removed, the professional shall refrain from dealing with the customer. Furthermore the professional shall, where applicable, consider filing a report with the State prosecutor.

Paragraph 5 Domiciled companies

60. In addition to this Circular, the professionals of the financial sector must also comply with all the legal obligations set out in circulars CSSF 01/28, CSSF 01/29, CSSF 01/47 and CSSF 02/65.

Sub-section 3 Obtaining information on the purpose and intended nature of the business relationship

61. The know-your-customer obligation requires the professional of the financial sector to collect more information on the customer than purely documentary evidence.

As a consequence, the entering into a business relationship with a new customer entails a judgement on the customer. This judgement has to be supported by obtaining information on the purpose and intended nature of the business relationship. Such information also allows the professional to understand the customer's professional or commercial activities as well as the risk profile.

62. This information should allow the professional of the financial sector to reduce the risk of being used for the purpose of money laundering or terrorist financing as far as possible and later to detect suspicious transactions due to their inconsistency with the information obtained.

Any unusual fact noticed during the identification process could be an indication of money laundering or terrorist financing and should as such prompt the professional of the financial sector to require further information.

Particular attention should be paid where the reasons given for seeking a business relationship are not clear or where the customer uses structures with no obvious economic purpose (tangle of accounts, misleading account names, etc.).

Sub-section 4 Conducting ongoing monitoring of the business relationship and keeping up-to-date the documents, data or information held

63. Professionals of the financial sector shall, in accordance with Article 3(2)(d) of the law of 12 November 2004 as amended, conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the professional's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

Paragraph 1 Ongoing monitoring of the business relationship

64. The professionals of the financial sector shall therefore implement a methodology to determine the degree of risk for every customer while targeting high-risk customers referred to in Article 3-2 of the law of 12 November 2004 as amended.

They are furthermore required to continuously monitor their customers from the beginning and throughout the entire business relationship. The extent of such measures can be adapted in accordance with the degree of risk of money laundering and terrorist financing associated

with the relevant customer. The professional shall also, in accordance with the risk assessment, know the source of the funds of the customer in question.

Customers referred to in points 80 to 94 shall be considered as high-risk customers (enhanced customer due diligence).

65. In order to be able to comply with the ongoing monitoring obligation of the business relationship, professionals of the financial sector should restrict the number of customers per account manager according to the type of customer and the technical systems and means.

Paragraph 2 Keeping up-to-date the documents and information held

66. At the time of the initial identification of the customer and verification of the identity based on a valid document, every professional of the financial sector had to check the customer's identity.

Identification is not invalidated by the fact that the document in question (e.g. ID card or passport) will eventually expire.

The professionals of the financial sector may thus rely on the identification and verification measures already performed, unless they have reason to doubt the veracity of the information obtained in the course of their monitoring of the business relationship. Suspicions of money laundering or terrorist financing with respect to a customer may arise where the transactions on a customer’s account change noticeably, in a manner that is inconsistent with the customer's activities or where the professional of the financial sector understands that information on the customer is insufficient. In such case, the professional of the financial sector may, following its assessment of the situation and the risk, update the identification file or renew the identification process.

Section 2 Obligation to pay special attention to certain activities and transactions

Sub-section 1 Transactions and operations potentially linked to money laundering or terrorist financing

67. In accordance with Article 3(7) of the law of 12 November 2004 as amended, the professional of the financial sector shall pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

68. In order to avoid being used for the purpose of money laundering or terrorist financing and to be able to detect suspicious transactions, the professionals of the financial sector must have a good understanding of the transactions requested by the customers. To this end, the professional of the financial sector shall carefully monitor the transactions carried out for

these customers and gather, where applicable, all the information necessary to remove any risk of money laundering or terrorist financing to a minimum.

69. Transactions involving low amounts but carried out at an unusually high frequency, high-risk transactions (e.g. linked to high-risk countries) and transactions that are unusual compared to the transactions normally carried out by the customer in question (e.g. unusual transaction compared to the usual operation of the account, transactions inconsistent with the declarations made when the account was opened, source and/or destination of the funds) also fall within the type of transaction referred to in point 67 above. Annexe II to this Circular lists examples of such transactions.

70. Contrary to the previous wording, Article 3(7) of the law of 12 November as amended no longer expressly refers to this issue, contrary to the previous wording in the law in this matter, nor to the circumstances surrounding a transaction or the type of persons involved, but only to the nature of the activity/transaction particularly likely to be linked to money laundering or terrorist financing The concept of the nature of an activity/transaction is however to be understood in the wider sense to include the notions of "type of persons involved" and "circumstances surrounding an activity/transaction". This provision should be read together with Article 5(1)(a) which deals with the relevant person, its development, origin of the monies, nature and purpose or procedure or the operation as being the criteria according to which the professional of the financial sector could have a suspicion of money laundering or financing of terrorism.

The monitoring of a transaction with respect to the type of persons involved covers both politically exposed persons residing abroad referred to in point 85 ff.of this Circular and persons (by way of nationality, place of activity or residence) from countries whose anti-money laundering and terrorist financing framework is considered as deficient at international level (see points 91 to 93 below).

71. Professionals of the financial sector shall take into account the specificities of combating terrorist financing, given that in such cases the process is often inverted compared to money laundering in that the funds originating from perfectly legal sources are injected into terrorist networks and systems.

72. Where, despite the efforts of the professionals of the financial sector to obtain the information enabling them to understand a transaction, doubts remain as to the absence of any link to money laundering or terrorist financing, yet without having a doubt as regards money laundering or terrorist financing, the professionals shall refuse to execute the transaction and even terminate the business relationship with the customer. If a matter arises which could indicate money laundering or financing of terrorism or which gives rise to a doubt, the professional shall make a report to the State prosecutor at the district court of Luxembourg (see points 118 ff. of this Circular).

Sub-section 2 Procedures, systems and mechanisms to implement in order to detect suspicious transactions

73. The professionals of the financial sector shall set up procedures and implement mechanisms and systems enabling them to detect both customers and beneficial owners recorded on official lists (e.g. list of terrorists) or private/internal lists (e.g. politically exposed persons (PEPs) residing abroad), as well as the funds from countries recorded on official lists (e.g. countries under embargo or countries referred to in points 91 and following) and dubious/suspicious transactions, given their abnormal or unusual nature or compared with the normal transactions of the customer concerned.
These mechanisms and systems shall be set up in co-operation with the anti-money laundering and terrorist financing officer.

74. Depending on the number of high-risk customers and transactions, it is recommended to set up a computer system that helps to detect transactions potentially linked to money laundering or terrorist financing, in order to ensure efficient monitoring of the transactions.

However, setting up an anti-money laundering computer system does not exempt the professionals of the financial sector from applying their anti-money laundering or terrorist financing policies by other means. The responsibility of the professional of the financial sector cannot be transferred to the designer of the software. Where such an anti-money laundering or terrorist financing computer tool is set up, this tool shall be configured under the supervision of the anti-money laundering and terrorist financing officer. Any voluntary or involuntary, inappropriate changes to the configuration, may indeed weaken, in the medium or in the long run, the efficiency of the computer tool in detecting money-laundering and terrorist financing transactions.

Sub-section 3 Written records of the results of the analyses performed

75. The professional of the financial sector shall document in writing the result of the review made on the activities/transactions considered as particularly likely to be linked to money laundering or terrorist financing.

Section 3 Obligation to keep certain documents and information

Subsection 1 Documents relating to the identification and verification of the identity

76. Documents relating to customer identification and verification of the identity of a customer shall notably include as regards natural persons:

- the account opening request form, signed and dated by the customer, detailing the customer's surname and first name, place and date of birth, nationality, full address, profession and reference number and date of the official identity document;
- where applicable, a copy of the official identity documents required for identification and verification of the identity;
- the documents relating to the verification of the identity of beneficial owners.

As regards companies and other legal persons, the documents shall notably include the account opening request form signed and dated by the representatives (proxies) indicated in point 42 above, including company name, legal form of the company or legal person, date of incorporation, full address of the registered office (and, where appropriate, if the company is a domiciled company, the seat of its domicile in Luxembourg), governing law, identity of the beneficial owner(s) and the documents pertaining to the verification of the identity of the beneficial owner(s) and the documents listed in points 40 to 42 of this Circular.

The professionals of the financial sector shall, as regards legal arrangements and trusts referred to in point 23, include in particular the account opening request form and all the documents which allowed them to understand the structure of the ownership and control of the customer.

Sub-section 2 Documents relating to transactions

77. The documents relating to transactions shall include notably:

- the transaction statement (nature and date of the transaction, transaction currency and amount, account type and number);
- the relevant correspondence;
- the contracts.

78. These documents must allow the reconstruction of individual transactions. The results of the reviews referred to in point 75 that the professional of the financial sector has to perform with respect to transactions that are particularly likely to be linked to money laundering or terrorist financing, shall also be recorded.

Subsection 3 Safekeeping of documents and information

79. Credit institutions and other professionals of the financial sector are required keep the documents and information mentioned in points 76 to 78 above to serve as evidence in any investigation into money laundering or terrorist financing or analysis of possible money laundering or terrorist financing by the Luxembourg authorities responsible for combating money laundering and terrorist financing.

In the case of customer due diligence, a copy or the references of the documents required shall be kept for a period of at least five years after end of the business relationship with their customer, without prejudice to longer record keeping periods prescribed by other laws.

In the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies certified in accordance to Luxembourg law, shall be kept for a period of at least five years following the carrying-out of the transactions or the end of the business relationship, without prejudice to longer record keeping periods prescribed by other laws.

Chapter 2 Enhanced customer due diligence

80. Professionals of the financial sector shall apply to their customers all the customer due diligence measures mentioned in Article 3 of the law of 12 November 2004 as amended and in this Circular. However, in situations which present a higher risk of money laundering or terrorist financing they shall furthermore apply enhanced measures for the identification and verification of the customer's identity.

Professionals shall apply enhanced customer due diligence on a risk-sensitive basis, in situations which by their nature can present a higher risk of money laundering or terrorist financing. They shall therefore analyse the risk factors which can be inherent to the specificity of their activity and their customers and set in place, where appropriate, such enhanced customer due diligence procedures.

Professionals shall pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

The examples described below are to be considered as high risk situations as a matter of course and therefore require the application of the specific enhanced customer due diligence measures. Professionals shall envisage the application of such measures in their internal procedures. Apart from these legal cases, this circular lists the case of the non-cooperative countries and territories and similar situations in which enhanced customer due diligence shall be applied.

Section 1 Non face-to-face entering into business relationships

81. Article 3-3 of the law of 12 November 2004 as amended firstly covers the situation where professionals of the financial section enter into a business relationship or execute a transaction on behalf of a customer who is not physically present for identification purposes. If so, the professional shall take specific appropriate measures to compensate the high risk of money laundering and terrorist financing which arises from this situation. These measures shall guarantee customer identification and verification of the customer's identity.

It should be noted that Article 3-1(4)(d) of the law of 12 November 2004 as amended also lists a specific example where simplified customer due diligence is justified given the low risk of money laundering or terrorist financing.

82. Professional have the choice to apply one of the following three types of measures before entering into the business relationship, however, according to their assessment of the customer's risk profile, they may apply more than one of these measures:

- measures ensuring that the customer's identity is established by additional documents, data or information (e.g. justification of the customer's professional activity; source of the funds, customer address etc);

- supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit institution.
  Professionals can thus require a copy of the customer's ID, certified by a competent authority (i.e. embassy, consulate, notary, police superintendent), or by a financial institution subject to equivalent regulation concerning the fight against money laundering and terrorist financing.

- measures ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.
  In this case the professional can require a simple copy of the customer’s ID document, as well as any other information required, as applicable, provided that the first transfer of funds is carried out through an account opened in the customer’s name with a credit institution which is subject to equivalent identification requirements.
  The CSSF accepts the procedure whereby the transfer order signed by the customer is directly sent by the Luxembourg bank to the customer’s bank bearing a reference number. On receipt of the transfer, the Luxembourg bank is able to verify by means of the account and reference numbers that the funds really originated from an account of the customer with the source bank. Any other procedure shall be subject to the CSSF's prior consent.

83. Moreover, professionals of the financial sector shall pay special attention to ensure receipt not only of all the documentation requested, but also of comprehensive and satisfactory answers to all the questions considered appropriate to ask in order to gain an informed understanding of the customer and of the purpose of the business relationship sought.

84. Prior to opening an account or executing a transaction, professionals of the financial sector shall review all the information provided by the customer, in accordance with their customer acceptance procedures.

Section 2 Politically exposed persons (PEPs)

85. In order to avoid implication in acts of money laundering, the professionals of the financial sector shall perform enhanced customer due diligence when seeking to enter into business relationships or to accept custody of assets belonging to, directly or indirectly, to PEPs residing in a foreign country.

Article 1(9) to (12) of the law of 12 November 2004 as amended provides important details regarding the concept of politically exposed persons.

86. Definitions

The law defines politically exposed persons (PEPs) as natural persons who are or have been entrusted with prominent public functions and immediate family members or persons known to be close associates of such persons. The definition is composed of three parts:

A) "Natural persons who are or have been entrusted with prominent public functions" means all natural persons, including:

a) heads of State, heads of government, ministers and deputy or assistant ministers;
b) members of parliament;
c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal except in exceptional circumstances;
d) members of courts of auditors or of the boards of central banks;
e) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
f) members of the administrative, management or supervisory bodies of State-owned enterprises.

According to the law, none of the categories set out in a) to f) above shall be understood as covering middle ranking or more junior officials.

The categories set out in a) to e) above shall, where applicable, include positions at Community and international level.

B) The Law of 12 November 2004 as amended defines "Immediate family members" as all natural persons, including:

a) the spouse;
b) any partner considered by national law as equivalent to the spouse. In general it means the laws which exist in certain countries regarding the domestic arrangements of two people co-habiting.

c) the children and their spouses or partners;
d) the parents.

C) "Persons known to be close associates" means all natural persons, including:
a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements together with a person who is or has been entrusted with a prominent public function, or to have any other close business relations with such a person;
b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of a person who is or has been entrusted with a prominent public function.

87. Applicable regime

Enhanced due diligence specifically designed for PEPs only applies in respect of transactions or business relationships with politically exposed persons residing in another Member State or in a Third Country, excluding PEPs residing in Luxembourg.

These measures shall be applied over and above the standard due diligence procedures laid down in Article 3 of the law of 12 November 2004 as amended and according to the degree of risk of money laundering or financing of terrorism by the specific customer. In this context, the professional shall set up special control policies and procedures, in order to have all the necessary guarantees when dealing with customers belonging to or joining the circle of the persons concerned.

The enhanced due diligence measure for PEPs shall be as follows:

a) have appropriate risk-sensitive procedures to determine whether the customer or the beneficial owner is a politically exposed person residing in a foreign country as defined in Article 1 of the law of 12 November 2004 as amended. The professionals of the financial sector shall thus set in place procedures, known to all the employees in contact with customers, enabling them, on a risk-sensitive basis, to detect PEPs as defined by the law. Such procedures consist of first and foremost the information in this matter received directly from the customer, of publicly available information or of information of commercial information databases on politically exposed persons;

b) obtain senior management approval prior to establishing business relationships with such customers.

   The anti-money laundering and terrorist financing officer should therefore be involved in the acceptance procedure of a PEP customer and authorisation by one of the managers duly authorised by law should be sought on a risk-sensitive basis, before entering into a business relationship with or executing an occasional transaction for such customer, taking into account the sensitivity of the matter.

c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction. The professional shall also, on a

risk-sensitive basis, verify the source of the funds and require documentary evidence;

d) conduct enhanced ongoing monitoring of the business relationship.

Without prejudice to other reasons justifying, as the case may be, the application of enhanced customer due diligence, where the person has ceased to be entrusted with a prominent public function for over one year, the professional of the financial sector shall in principle not be obliged to consider such a person as politically exposed.

It ought to be stressed that the requirement to also identify as PEPs close associates of natural persons who are entrusted with prominent public functions, shall only apply to the extent that the relation with the associate is publicly known or that the professional has reasons to believe that such relation exists. Thus it does not presuppose active research on the part of the professional.

The definition of PEP implies that essentially persons exercising important functions at a national level of a State are contemplated. Public functions exercised at levels lower than national i.e. regional or local level, are normally not considered to be prominent. However, where their political exposure is comparable to that of similar positions at national level, professionals of the financial sector should assess, on a risk-sensitive basis, whether persons exercising those public functions (abroad) should be considered as PEPs.

88. Please note that the ensuing business relationship shall also be closely monitored by the professional and specifically by the anti-money laundering and terrorist financing officer, in compliance with point d) above.

Section 3 Correspondent banks

89. Article 3-2(3) of the law of 14 November 2004 as amended requires credit institutions, in case of cross-border relation correspondent banking relationships with a respondent institution from a third country which does not figure on the list of "third countries which impose equivalent requirements" published by way of Grand-ducal regulation of 29 July 2008 mentioned above to:

a) gather sufficient information about the customer institution to understand fully the nature of the respondent's business and to determine from publicly available information, the reputation of the institution and the quality of the supervision it is subject to;

b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls;

c) obtain approval from senior management before establishing new correspondent banking relationships;

d) document the respective responsibilities of each institution;

e) with respect to *payable-through accounts*, be satisfied that the customer credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

In this context, the law of 12 November 2004 as amended expressly prohibits credit institutions to enter into or continue a correspondent banking relationship with a shell bank or with a bank that is known to permit its accounts to be used by a shell bank. A shell bank is a credit institution, or an institution engaged in equivalent credit institution activities, incorporated in a jurisdiction in which it has no physical presence, that would involve meaningful administration and management, and which is unaffiliated with a regulated financial group.

90. Aside from the situations laid down by law which require the application of enhanced due diligence, other situations can exist, such as the situation of non-cooperative countries and territories and similar situations implicating customers from countries or territories (by way of nationality, place of activity or residence) whose anti-money laundering and terrorist financing framework is considered as deficient by the FATF.
Furthermore, customers can also become high-risk customers due to their behaviour, in particular with respect to executed transactions.

Section 4 Non-cooperative countries and territories (NCCTs) and similar situations

91. The FATF publishes declarations which bring to light deficiencies in the anti-money laundering or terrorist financing of the designated countries. These declarations, which are not the same as the mutual evaluation reports drawn up by the FATF, are addressed to professionals of the financial sector so that they take into consideration the risks resulting from the stated deficiencies of these anti-money laundering/counter-terrorist financing regimes by applying enhanced customer due diligence. These declarations are available on the FATF website: www.fatf-gafi.org

92. With this new approach the FATF replaces the list it used to publish on non-cooperative countries and territories (NCCTs) as regards the fight against money laundering and terrorist financing, i.e. of those jurisdictions the anti-money laundering and terrorist financing legislation and regulations of which are considered not to comply with the FATF recommendations as well as a second list which details the NCCTs against who counter-measures have been decided on the basis that they to not make sufficient effort to improve their framework in the fight against money laundering and terrorist financing. These specific lists no longer include any countries so that one should take into account only the declarations referred to in point 91 above.

93. Professionals of the financial sector shall, on a risk-sensitive basis:

- set up acceptance and transaction monitoring policies and procedures as regards relations with counterparties located in countries referred to in the FATF declarations, be they natural or legal persons, including professionals of the financial sector. Enforcement of this policy shall be monitored by the anti-money laundering and terrorist financing officer;

- in particular, apply enhanced identification procedures. In this context, the origin of the funds shall be verified (at the slightest doubt or uncertainty, supporting evidence shall be required) and the professional of the financial sector shall obtain from the stated beneficial owner written confirmation of his ownership;

- involve the anti-money laundering and terrorist financing officer in the acceptance procedure of such customers and to consider, if applicable, on a risk-sensitive basis, the authorisation of one of the executive officers duly authorised as required by law, before entering into a business relationship with or executing a transaction for such customers, taking into account the sensitivity of the matter;

- examine with due attention the transactions involving counterparties located in countries referred to in the FATF declarations, be they natural or legal persons, including professionals of the financial sector, or the transactions relating to funds from such countries or territories.

94. The external auditor shall verify compliance with the relevant internal procedures and specifically refer thereto in the long-form report.

Chapter 3 Performance of customer due diligence by third parties

95. The performance of customer due diligence laid down in Article 3(2) (a) to (c) of the law of 12 November 2004 as amended, does not necessarily have to be done by the professionals of the financial sector themselves. These measures can, under certain conditions, be performed by third parties. The performance of customer due diligence by third parties thus avoids the repetition of the customer identification procedures and, as the case may be, delays in the execution of transactions.

96. The law of 12 November 2004 as amended allows professionals of the financial sector to accept, under certain conditions, customers for whom due diligence was performed by a third party (art. 3-3 (1) to (4)) (**third party** regime). The law also allows the delegation of the performance of due diligence to third parties by way of contract (art. 3-3(5)) (**outsourcing**).

It should be borne in mind that only the physical process of customer due diligence may be performed by a third party but that the final decision as to whether a business relationship is established falls to the professionals of the financial sector themselves.
At the same time, the ultimate responsibility for performing the due diligence obligations remains with the professionals which rely on the third party. The professionals of the financial sector may not delegate this responsibility thereby eluding their obligation to know their customers.

Third parties performing due diligence retain their own responsibility for all the requirements in the law of 12 November 2004 as amended, including the requirement to report suspicious transactions to the competent authorities and keep records, to the extent that they have a relationship with the customer covered by this law.

Section 1 Third party regime

97. Art. 3-3 (1) to (4) of the law of 12 November 2004 as amended defines the condition on which professionals of the financial sector may accept customers for whom identification was already performed by a third party.

Sub-section 1 Accepted third parties

98. Accepted third parties from Luxembourg: Article 3-3(1) of the law of 12 November 2004 as amended provides that a limited number of specific professionals can act as third parties, namely the following Luxembourg professionals:

a. credit institutions and other professionals of the financial sector (PFS) licensed or authorised to exercise their activites in Luxembourg in accordance with the law of 5 April 1993 on the financial sector as amended;
b. insurance undertakings licensed or authorised to exercise their activities in Luxembourg in accordance with the law of 6 December 1991 on the insurance sector, as amended, in connection with operations covered by point 11 of the Annexe of the

law of 6 December 1991, as amended, and insurance intermediaries licensed or authorised to conduct business in Luxembourg in accordance with the law of 6 December 1991 on the insurance sector, as amended, where they act in respect of life insurance and other investment related services;

c. undertakings for collective investment and investment companies in risk capital (SICAR), which market their units or shares and to which the law of 20 December 2002 relating to undertakings for collective investments, as amended, or the law of 13 February 2007 on specialised investment funds or the law of 15 June 2004 relating to the investment company in risk capital (SICAR) applies;
d. management companies under the law of 20 December 2002 as amended on undertakings for collective investment which market units/shares of UCIs or perform additional or auxiliary activities within the meaning of the law of 20 December 2002 as amended relating to undertakings for collective investment;
e. auditors, within the meaning of the law of 28 June 1984 on the organisation of the profession of company auditors, as amended;
f. notaries, within the meaning of the law of 9 December 1976 on the organisation of the profession of notaries, as amended;
g. lawyers, within the meaning of the law of 10 August 1991 on the legal profession, as amended when acting in the cases listed in Article 2(1)12. (a) to (c) of the law of 12 November 2004 as amended.

99. Accepted Third parties from other Member States of the European Union or the European Economic Area.

The following persons are concerned:

a. credit and financial institutions of other Member States as defined in Article 3 of Directive 2005/60/EC;
b. legal and natural persons (acting in the exercise of their professional activities) from other Member States as defined in Article 2 (1) (3) (a) to (c) of Directive 2005/60/EC, i.e.
    i. auditors, external accountants and tax advisors;
    ii. notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the: i) buying and selling of real property or business entities; ii) managing of client money, securities or other assets; iii) opening or management of bank, savings or securities accounts; iv) organisation of contributions necessary for the creation, operation or management of companies; v) creation, operation or management of trusts, companies or similar structures;
    iii. trust or company service providers not already covered under points i) or ii) above.

These third parties must fulfil each of the following conditions:

1. they are subject to mandatory professional registration, recognised by law;
2. they apply customer due diligence and record keeping requirements as laid down in Directive 2005/60/EC;
3. they are subject to the supervision provided for in Section 2 of Chapter V of Directive 2005/60/EC as regards compliance with the provisions of Directive 2005/60/EC.

Conditions 1-3 above are fulfilled ipso jure for the persons referred to in point a) above which are subject to prudential supervision in keeping with the requirements of Directive 2005/60/EC.

100. Accepted third parties of third countries:

Institutions or persons equivalent to those listed in point 99 above, which are situated in a third country (other than a Member State of the European Union or of the European Economic Area) listed in Grand–ducal Regulation of 29 July 2008 establishing the list of "third countries which impose equivalent requirements" within the meaning of the law of 12 November 2004 as amended, may also perform customer due diligence provided they fulfil each of the following conditions:

1. they are subject to mandatory professional registration, recognised by law;
2. they apply customer due diligence and record keeping requirements as laid down, or equivalent to those laid down, in the law of 12 November 2004 as amended or in Directive 2005/60/EC;
3. they are subject to supervision which is equivalent to that laid down in Section 2 of Chapter V of Directive2005/60/EC.

Sub-section 2 Conditions

101. In accordance with Article 3-3(2) and (3) of the law of 12 November 2004 as amended, professionals relying on third parties for the performance of the due diligence obligations have to make sure from the start that their involvement in the obtaining of required documents and information is assured.

Where the third party is situated abroad, professionals of the financial sector have to make sure that the former agrees to get involved and will immediately make the required information available, without objecting to any rules of confidentiality or professional secrecy, in accordance with the requirements laid down in Article 3(2) (a) to (c) of the law of 12 November 2004 as amended and will, upon request and without delay, provide an adequate copy of the identification and verification data as well as any other relevant document relating to the identity of the customer and of the beneficial owner.

Where Luxembourg professionals are unable to obtain the required documents or information without delay in order for them to be used *inter alia* in the context of a request

from the competent authorities concerning the fight against money laundering and terrorist financing, this constitutes a breach of their professional obligations.

In case the third party is situated in Luxembourg, Article 3-3 (2) and (3) of the law of 12 November 2004 as amended has to apply necessarily to the professional and the obligation to provide the relevant information or documents derives directly from this Article.

According to Article 3-3 (4) of the law of 12 November 2004 as amended, where the customer due diligence is carried out by a third party situated abroad in accordance with Article 3(2)(a) to (c) of the law of 12 November 2004 as amended or with Directive 2005/60/EC, the outcome of the due diligence performed abroad is recognised and accepted in Luxembourg, even if the documents or data on which the due diligence was based are different from those required in Luxembourg.

Section 2 Outsourcing

102. Article 3-3(5) of the law of 12 November 2004 as amended provides that the third party regime described in points 97 to 101 above can be distinguished from the situation where professionals outsource or delegate certain duties by way of contract to other trusted persons not subject to the law of 12 November 2004 as amended or to equivalent regulation concerning the fight against money laundering and terrorist financing. Where customer due diligence measures are outsourced, the delegated agent or outsourcing service provider is said to merge with the professional to the extent that the applicable measures are those of the professionals themselves.

103. Whereas 28 of Directive 2005/60/EC provides that where a contractual agency or outsourcing relationship exists between professionals subject to the law of 12 November 2004 as amended and external natural or legal persons not subject to the law or said Directive, the obligations relating to the fight against money laundering or terrorist financing which fall upon the agent or the outsourcing service provider can only derive from the contract and not from the law of 12 November 2004 as amended. Even in cases where Article 3-3 does not apply, the full responsibility pursuant to the law of 12 November 2004 as amended clearly remains with the professionals. The latter shall ensure, by the choice of counterparty and by the terms of the contracts, that adequate guarantees are in place which allow them to comply with the obligations of the law.

Professionals, having chosen a trustworthy counterparty in terms of performance of their due diligence obligations, still have to sign a written contract with the counterparty. The contract may be by separate letter in which the delegate undertakes vis-à-vis the professional of the financial sector to observe all the obligations contained on a detailed list.

The outsourcing contract must specifically define the delegated tasks taking into account the requirements laid down by the law of 12 November 2004 or Directive 2005/60/EC as well as by this Circular.

The contract has to include at least a detailed description of the due diligence measures (including simplified and enhanced due diligence measures) which the third party has to carry out in accordance with the law of 12 November 2004 as amended and it has to describe specifically which information and documents the third party has to request and to verify. The contract has to include the terms and conditions relating to the communication of information and documents required by the Luxembourg professionals. Thus, the Luxembourg professionals have to be sure that the delegated third party will immediately make the required information available, without opposing any rules of confidentiality or professional secrecy or any other obstacle, and will, upon request and without delay, provide an adequate copy of of the original identification and verification data as well as any other relevant document relating to the identity of the customer and, if applicable, of the beneficial owner. These documents consist of the official identification document and the account opening form printed on headed notepaper of the Luxembourg institution and contain all other information required to fulfil the know-your-customer obligation (purpose of the business relationship, professional activity, beneficial owner and, where applicable, the source of funds).

The copies shall be certified true to the original by the delegates or the authorised persons when entering into a non face-to-face relationship in accordance with points 81 to 84 of this Circular. The Luxembourg professionals shall not accept a certificate drawn up by a third party, irrespective of his/her status, stating that this third party knows the identity of the customer, has verified it and holds the required documentation.

104. The internal procedures of those professionals wishing to appoint a third party or a proxy shall also include detailed provisions regarding the applicable regime. As regards in particular outsourcing, the procedures have to include provisions relating to the choice of delegated agent so that the professional can rest assured that the agent will fulfil his/her obligations contained in the outsourcing or agency contract.

Chapter 4 Simplified customer due diligence

105. In principle, professionals have to systematically apply the measures laid down in Article 3 of the law of 12 November 2004 as amended, even if they can adapt the extent of the measures in Article 3(2) according to their risk assessment.

Nevertheless, in order to take into account situations where the risk of money laundering or terrorist financing is low, the law of 12 November 2004 as amended lists a number of situations in which professionals are exempt from performing the due diligence measures laid down in Article 3(2) and the first paragraph of Article 3(2)(4), unless there is a suspicion of money laundering or terrorist financing. In practice, the biggest effect of the simplified due diligence will be on the degree of the beneficial owner identification and verification of identity which professionals can in principle dispense with.

106. However it should be stressed that the simplified regime does not exempt Luxembourg professionals from all due diligence obligations.

Thus, in accordance with Article 3-1(3) professionals shall always first gather sufficient information to assess whether the simplified due diligence measures can actually be applied in the case at hand.

In certain cases professionals then have to first make sure that the customer, the products or the transactions in question actually do present a low risk of money laundering or terrorist financing before the simplified due diligence can be applied (Article 3-1(5) of the law of 12 November 2004 as amended). The obligation of prior assessment before applying simplified due diligence does not exist in every case, only in the circumstances listed in paragraph (2)(d) and (e) and in paragraph (4)(e) of Article 3-1. During this assessment, professionals shall pay special attention to any activity of those customers or any type of product or transaction which may be regarded as particularly likely, by its nature, to be used or misused for money laundering or terrorist financing purposes. Professionals are not authorised to perform simplified due diligence if this prior risk assessment does not show that the risk is actually low. In this case, professionals shall apply all the due diligence measures foreseen in Article 3 and might even have to apply enhanced due diligence if the risk turns out to be high.

The simplified due diligence regime is further ruled out in case of suspicion of money laundering or terrorist financing within the meaning of Article 3(1)(c) of the law of 12 November 2004 as amended. If so, a suspicious transaction report shall be made to the State prosecutor in accordance with Article 5 of the law of 12 November 2004 as amended.

The performance of simplified customer due diligence does not exempt professionals of the financial sector of the other requirements in the fight against money laundering or terrorist financing, notably monitoring transactions and co-operating with the authorities, required by law with respect to all their customers.

107. The obligations laid down in Article 3-1(1) of the law of 12 November 2004 as amended shall not apply to professionals where the customer:

- is a Luxembourg credit or financial institution subject to the law of 12 November 2004 as amended, or
- is a credit or financial institution within the meaning of Article 3 of Directive 2005/60/EC which refers to another Member State of the European Union or the European Economic Area, or
- is a credit or financial institution incorporated in a third country and included on the list laid down in Grand–ducal Regulation of 29 July 2008 establishing the list of "third countries which impose equivalent requirements" within the meaning of the law of 12 November 2004 on the fight against money laundering and terrorist financing as amended and is subject to supervision in this respect.

As regards these customers, in particular those from third countries, Luxembourg professionals shall first check that the customer actually is a credit or financial institution as

described above. This requirement includes but is not limited to making sure that the customer is not a shell bank in accordance with Article 3-2 (5).

Where the customer of the professional of the financial sector is a UCI that do not market its units/shares itself, a management company or a pension fund as referred to in point 15 of this Circular, it must be identified by means of its articles of incorporation.

108. The condition of equivalence is also fulfilled by branches or subsidiaries of credit or financial institutions from another Member State of the European Union or of the European Economic Area or a third country included on the list published by the Grand-ducal regulation of 29 July 2008, irrespective of the country in which they are located, provided that the institutions concerned require their branches and subsidiaries to comply with the provisions applicable to them, either by virtue of a legal provision or of a group rule.

109. The performance of simplified customer due diligence is not allowed if the customer to whom the simplified due diligence measures apply pursuant to Article 3-1 of the law of 12 November 2004 as amended, only introduces one or more customers to a professional of the financial sector. Indeed, if the customer is not such a customer pursuant to the above-mentioned Article, he/she must be identified by the professional of the financial sector with whom he/she enters into a business relationship on a non face-to-face basis where applicable, or in the context of the identification by a third party, in compliance with the applicable provisions.

110. The instances in which Luxembourg professionals may refrain from perfuming customer due diligence are detailed in Articles 3(1) (2) and (4) of the law of 12 November 2004 as amended.

The cases concerned are the following:

a) companies whose securities are admitted to trading on a regulated market within the meaning of Article 1(11) of the law of 13 July 2007 on markets in financial instruments in one or more Member States and listed companies from Third Countries which are subject to disclosure requirements consistent with Community legislation, i.e. Commission Directive 2007/14/EC of 8 March 2007 laying down detailed rules for the implementation of certain provisions of Directive 2004/109/EC on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market;

b) beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions acting as depository institutions for the pooled accounts (see also points 54 to 56 of this Circular).

c) Luxembourg public authorities.
The simplified customer due diligence regime is thus not applicable to public authorities from a foreign state.

d) customers (who are not natural persons) who are public authorities or public bodies representing a low risk of money laundering or terrorist financing and who fulfil all the following criteria:
- the customer has been entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation;
- the identity of the customer is publicly available, transparent and certain;
- the activities of the customer, as well as their accounting practices, are transparent;
- either the customer is accountable to a Community institution or to the authorities of a Member State, or appropriate check and balance procedures exist ensuring control of the customer's activity;

e) customers other than those referred to under d) above, who are legal persons representing a low risk of money laundering or terrorist financing and who satisfy all the following criteria:
- the customer is an entity that undertakes financial activities outside the scope of Article 2 of Directive 2005/60/EC but who is subject to legislation which has applied the obligations of said Directive. Such entity shall include subsidiaries only in so far as the obligations of Directive 2005/60/EC have been extended to them on their own account;
- the identity of the customer is publicly available, transparent and certain;
- the customer is subject to a mandatory licensing requirement under national law for the undertaking of financial activities and licensing may be refused if the competent authorities are not satisfied that the persons who effectively direct or will direct the business of such an entity, or its beneficial owner, are fit and proper persons. For these purposes, the activity conducted by the customer shall be supervised by competent authorities. "Supervision" is to be understood in this context as meaning the type of supervisory activity with the highest supervisory powers, including the possibility of conducting on-site inspections. Such inspections shall include the review of policies, procedures, books and records, and shall extend to sample testing:
- the customer is subject to supervision by competent authorities as regards compliance with the national legislation transposing that Directive and, where applicable, additional obligations under national legislation;
- failure by the customer to comply with the obligations referred to in the first indent of this point e) is subject to effective, proportionate and dissuasive sanctions including the possibility of appropriate administrative measures or the imposition of administrative sanctions.

It should be stressed that in all the cases mentioned above, professionals shall in any case gather sufficient information to establish if the customer qualifies for an exemption.

111. The law of 12 November 2004 as amended also sets out the option to apply simplified customer due diligence in case of investment into certain products or transactions presenting a low risk of money laundering or terrorist financing.

The cases concerned are the following:

a) life insurance policies where the annual premium is no more than EUR 1,000 or the single premium is no more than EUR 2,500;

b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

d) electronic money, as defined in Article 12(10) of the law of 5 April 1993 on the financial sector, as amended where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where, if the device can be recharged, a limit of EUR 2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1,000 or more is redeemed in that same calendar year by the bearer as referred to in Article 12(12) of the law of 5 April 1993 on the financial sector, as amended;

e) other products or transactions related to such products representing a low risk of money laundering or terrorist financing and which satisfy all the following criteria:

- the product has a written contractual base;
- the related transaction is carried out through an account of the customer with a credit institution of a Member State or a credit institution situated in a Third Country which imposes requirements equivalent to those laid down by the law of 12 November 2004 as amended or by Directive 2005/60/EC;
- the product or related transaction is not anonymous and its nature is such that it allows for the timely application of Article 3(1)(c);
- the product is subject to a predetermined maximum threshold of EUR 15,000, subject to the derogations below.
  In the case of insurance policies or savings products of similar nature the thresholds established in a) of paragraph of this point 111 apply.
  In the case of products which are related to the financing of physical assets and where the legal and beneficial title of the assets is not transferred to the customer until termination of the contractual relationship, the threshold established under this point 111 a) for transactions related to this type of product may be exceeded, whether the transaction is carried out in a single operation or in several operations which appear to be linked, provided it does not exceed EUR 15,000 per year.
- the benefits of the product or related transactions cannot be realised for the benefit of third parties, except in the case of death, disablement, survival to a predetermined advanced age, or similar events;
- in the case of products or related transactions allowing for the investment of funds in financial assets or claims, including insurance or other kinds of contingent claims:
  i) the benefits of the product or related transactions are only realisable in the long term;

ii) the product or related transaction cannot be used as collateral;
iii) during the contractual relationship, no accelerated payments are made, no surrender clauses are used and no early termination takes place.

Chapter 5 Adequate internal management requirements

112. Pursuant to Article 4 (1), (2) and (3) of the law of 12 November 2004 as amended, the professionals of the financial sector shall:

- establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.

- take adequate and appropriate measures to make their relevant employees aware of and train them as regards the provisions concerning the professional obligations in the fight against money laundering and terrorist financing applicable to them. These measures shall include participation of the relevant employees in special ongoing training programmes to help them recognise operations that may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

- have systems in place that enable them to respond fully and rapidly to enquiries from the Luxembourg authorities responsible for combating money laundering and terrorist financing as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

These procedures and measures shall be established by each professional taking into account the particularities of their activities and their differences in scale and size and controlled in accordance with the provisions set down in point 3 above. They are required to communicate the relevant policies and procedures, where applicable, to branches and subsidiaries referred to in Article 2(2) of the law of 12 November 2004 as amended.

Section 1 Obligation to establish written internal control and communication procedures

113. Each professional of the financial sector shall adopt a programme on the fight against money laundering and terrorist financing, focusing on the internal policies, procedures and controls which are necessary to comply with each of the professional obligations arising from the law of 12 November 2004 as amended. It is important that the professionals adjust these procedures taking into account the particularities of their respective activities and their differences in scale and size. The procedures shall also appoint an anti-money laundering and terrorist financing officer as well as set up adequate procedures relating to the hiring of employees.

To this end, professionals of the financial sector shall have a regularly-updated, precise and comprehensive procedures manual, comprising notably:

- the detailed description of the procedures to be followed as regards the content and form, when entering into a business relationship with a customer or executing transactions for occasional customers, according to type of business relationship or transaction, and according to type of customer (private individual, retailer, commercial company, holding company, etc.).

  The procedures shall include a description and justification of the situations giving rise, as the case may be, to an adjustment to the extent of applicable due diligence measures given the professional's assessment related to the type of client, the business relationship, the product or transaction in question based on Article 3(3) of the law of 12 November 2004 as amended. The performance of simplified due diligence can be envisaged and enhanced measures shall be applied for the situations, customers, products or transactions referred to notably in points 80 and following above.

  The procedures shall also include measures designed to prevent the use of the products or the execution of transactions that might favour anonymity pursuant to Article 3-2(6) of the law of 12 November 2004 as amended, in particular in the context of new technologies. Professionals shall, where applicable, have in place specific risk management mechanisms relating to business relationships or transactions not requiring the physical presence of the parties.

- the detailed description of the procedures to be followed, as regards the content and form, where the professional of the financial sector receives a request to enter into a business relationship or to execute an occasional transaction for a person (e.g. a lawyer or a notary) whose normal professional activity includes the holding of third-party funds with a professional of the financial sector or to open a pooled account.
  Point 54 of this Circular specifies that the professional of the financial sector shall expressly ask such persons whether they act on their own behalf or on behalf of others and must assess the plausibility of the response given.

- the detailed description of the procedures to be followed, with respect to the content and form, where a professional knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being committed;

- the detailed description of the procedures to be followed, with respect to the content and form, where a fact that could be an indication of money laundering or terrorist financing is detected and comes to the attention of the professional of the financial sector while performing his/her professional activities without a business relationship being established or a transaction executed. The procedures shall require that all contacts be documented, whatever the form such contacts takes. The notion of “entering into contact” with a customer includes any possible form of contact, including contact by post, phone conversation or electronic means (such as the Internet). The procedures to be applied by the professionals of the financial sector must be adapted according to the

different possible forms of contact and in particular comprise the appropriate questions professionals of the financial sector shall ask according to the form of contact concerned and the degree of intensity of the contact.
The professionals of the financial sector shall document all indications of money laundering and terrorist financing that have come to their attention within the context of their commercial contacts.
The documentation must contain all the information that the professionals of the financial sector obtained on the person who they entered into contact with. Furthermore, it must state the reasons for the professional of the financial sector's refusal to establish a business relationship or to execute the transaction concerned for this potential customer. Where the professional of the financial sector's decision not to enter into a business relationship or not to execute a transaction is not based on a fact relating to an indication of money laundering or terrorist financing, this decision shall also be documented as far as possible.

- the detailed description of the procedures to be followed, with respect to the content and form, to monitor the transactions executed for their customers in order to detect suspicious transactions.
  Special procedures must be implemented to ensure reinforced monitoring of high-risk customers, including notably those referred to in points 80 and following above.

- the detailed description of the procedures to follow, with respect to the content and form, to comply with the obligation to report to the CSSF, concomitant to the communication of information to the State prosecutor in accordance with Article 5(1) of the law of 12 November 2004 as amended, the same information as that communicated to the State prosecutor;

- the detailed description of the procedures to be followed, with respect to the content and form, where the professional of the financial sector performs non face-to-face transactions;

- the exact definition of the respective responsibilities of all the employees involved in these procedures.

Section 2 Obligation to train and inform employees

114. Professionals of the financial sector shall set up a training and information programme for their employees, which is adapted to the development of money-laundering and terrorist financing techniques and which comprises notably:

- a specific ongoing training programme of courses held at regular intervals, in particular to employees that are in direct contact with customers, in order to help them recognise operations related to money laundering or terrorist financing and to instruct them as to how to proceed;

- regular information meetings for employees to keep them abreast of the preventive rules and procedures to follow in the context of the fight against money laundering or terrorist financing;

- the appointment of one or several competent persons able to respond at any time to the questions of other employees on money laundering or terrorist financing;

- the systematic distribution of money-laundering and terrorist financing documentation, providing notably examples of money-laundering or terrorist financing operations, such as the list of indications of money laundering appended to this Circular.

115. Where the professionals of the financial sector adopt procedure manuals and information programmes developed abroad, e.g. by their head office or parent company, they are required to adapt these procedures and programmes to the rules applicable in Luxembourg.

Section 3 Obligation to have systems in place that enable to respond to enquiries from the Luxembourg authorities

116. Credit and financial institutions shall, in accordance with Article 4(3) of the law of 12 November 2004 as amended, have systems in place that enable them to respond fully and rapidly to enquiries from the Luxembourg authorities responsible for combating money laundering and terrorist financing as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

It is important that the professionals under this obligation are able to respond rapidly and fully to the enquiries from the Luxembourg authorities responsible for combating money laundering and terrorist financing relating to current or past business relationships they held with named persons, including such persons included on the list of suspicious persons with respect to the fight against terrorism and its financing.

In order to identify such business relationships and to be able to provide information rapidly in response to such enquiries, professionals shall have effective systems in place which are commensurate with the size and nature of their business. In particular it is recommended for credit institutions and larger financial institutions to have electronic systems at their disposal which allow them to detect such persons.

These electronic systems are also important in the context of procedures leading to measures such as the freezing or seizing of assets, pursuant to applicable national or Community legislation.

It is hereby stressed that the procedures relating to the use of third parties for the performance of due diligence have to allow a good cooperation with the Luxembourg authorities responsible for combating money laundering and terrorist financing.

Chapter 6 Obligation to co-operate with the authorities

Section 1 General obligation to co-operate with the law enforcement authorities

117. Pursuant to Article 40 of the law of 5 April 1993 on the financial sector as amended, the professionals of the financial sector are obliged to respond and co-operate as comprehensively as possible with respect to any legal request received from the law-enforcement authorities, issued in the exercise of their duties.

Section 2 Obligation to co-operate with the Luxembourg authorities responsible for combating money laundering and terrorist financing

118. Pursuant to Article 5 of the law of 12 November 2004 as amended, the professionals of the financial sector, their directors and employees are obliged to co-operate fully with the

Luxembourg authorities responsible for combating money laundering and terrorist financing.

Sub-section 1 Obligation to provide to the State prosecutor at the Luxembourg district court , upon his request, all the required financial information

119. Pursuant to Article 5 (1), the professionals of the financial sector shall fully co-operate with the State prosecutor by promptly providing, upon his request, all necessary information. Please also note that in this case the obligation as regards professional secrecy is lifted.

It is worth repeating, in this context, that professionals have to comply with the procedures they shall put in place pursuant to Article 4(3) of the law of 12 November 2004 as amended and referred to in point 116 above.

Sub-section 2 Obligation to inform, on its own initiative, the State prosecutor at the Luxembourg district court of any suspicion or fact of money laundering or terrorist financing

Paragraph 1 Persons responsible of informing the State prosecutor

120. The communication of information to the State prosecutor, upon his request or on the initiative of the professional of the financial sector, shall be taken care of by the anti-money laundering and terrorist financing officer in accordance with the internal procedures that the professionals of the financial sector are required to set up. It should be borne in mind that this officer must be the compliance officer as far as credit institutions and investment firms are concerned. As regards the other professionals of the financial sector, this officer shall be a manager duly authorised by law.

It should be stressed that the identity of the employees of the professional who have provided such information is kept confidential by the competent authorities, unless disclosure is essential to ensure the regularity of legal proceedings or to establish proof of the facts forming the basis of these proceedings.

121. Every professional of the financial sector is required to inform the CSSF of the name of the persons designated to the State prosecutor as being responsible for communicating information to the State prosecutor. These persons shall also be the contact persons of the CSSF for any question relating to money laundering or terrorist financing.

122. In this context, the State prosecutor of the district court of Luxembourg, being competent in this field for the entire territory of the Grand Duchy of Luxembourg, has issued a circular to all professionals of the financial sector in order to set down the practical considerations regarding the information to provide to the State prosecutor (Circular 20/08 CRF of 12 November 2008).

Paragraph 2 Circumstances in which the State prosecutor must be informed

123. This point purports to clarify the approach to be adopted by professionals of the financial sector when confronted with a suspicious situation or person, in order to inform them of the risks they may incur and to reassure them in their way to proceed. Indeed, in the event of an inopportune report, the professionals run the risk of being accused by the customer of violating their professional secrecy obligation. Conversely, they run the risk of criminal proceedings should they refrain from filing a report under circumstances covered by Article 5 of the law of 12 November 2004 as amended.

Pursuant to Article 5(1) a) of the law of 12 November 2004 as amended, professionals shall promptly file a report with the State prosecutor, where professional know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing is being committed or has been committed or attempted. Furthermore, professionals shall file a report with the State prosecutor where they know i.e. have certainty that such is the case.

I. Clarification of the criteria to be considered in the detection of money laundering or terrorist financing

124. The above-mentioned Article 5(1)a) specifies the criteria (person concerned, development of the customer, source of the funds, nature, purpose or terms of the transaction) that should be taken into account in order to assess whether there is a suspicion of money laundering or terrorist financing. Furthermore, a non-exhaustive list of money-laundering indicators is presented in Annexe II to this Circular.

125. In order to inform the professionals of the financial sector of the scope of the money-laundering and terrorist financing offence, as well as of the scope of the reporting obligation, the list of the predicate offences at point 8 above is split into the categories of predicate offences laid down by the FATF.

126. Within the context of combating terrorist financing, professionals of the financial sector shall also report to the State prosecutor those transactions that involve persons mentioned in the official lists of presumed terrorists or terrorist organisations (see Annexe III).

II. Clarification of the obligation to inform as regards the fight against money laundering and terrorist financing

127. Where professionals know, suspect or have reasonable grounds to suspect that money laundering or terrorist financing is being committed or has been committed or attempted, they shall promptly file a report with the State prosecutor at the district court in Luxembourg. A suspicion may arise in view to the person concerned, its development, origin of the monies, nature and purpose or terms of the operation.

Where professionals of the financial sector face a situation which might give rise to a suspicion of money laundering or financing of terrorism, they have to check whether the funds underlying one or more transactions are likely to stem from one of the predicate offences referred to in point 8 of this Circular. Consequently, in order to determine whether

or not a declaration has to be filed pursuant to Article 5(1)(a), the professional of the financial sector shall seek to clarify the situation, notably by questioning the customer on the source of the funds and by inviting him/her to provide any useful additional information.

128. The professional of the financial sector will then assess the plausibility of the explanations provided. In the case of contacts with PEPs residing abroad referred to in points 85 to 88, the professional shall consider involving the anti-money laundering and terrorist financing officer. Where such approach does not permit the satisfactory clarification of the situation or where professional of the financial sector are personally convinced that the suspicion is justified, they are obliged to promptly report the fact to the State prosecutor at the district court of Luxembourg. It is hereby clarified that the obligation to promptly inform the State prosecutor at the district court in Luxembourg arises from the moment where the professional knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being committed or has been committed or attempted.

129. However, the professional of the financial sector need not penally classify the facts nor prove their accuracy. This task falls to the competent judicial authorities.

130. The professional's approach shall be the same with respect to facts that have been committed abroad.

III. Specifications concerning the obligation to inform in the event of a first contact without entering into a business relationship and/or without making a transaction

131. Where there is an indication of money laundering or terrorist financing, the obligation to inform the State prosecutor, as provided in Article 5 of the law of 12 November 2004 as amended, also covers situations where the professional of the financial sector entered into contact with a person or a company without a business relationship being entered into or a transaction executed.
In this event, professionals shall document every piece of information obtained on the person who entered into contact with them, as well as all indications of money laundering or terrorist financing which came to their attention as a result of this contact.

132. No report needs to be filed where the decision not to enter into a business relationship or execute a transaction is not based on an indication of money laundering or terrorist financing.
If so, the reasons underlying the formal refusal of the professionals' officer or body empowered to authorise a new business relationship shall also be documented as far as possible, together with the information that the professional has obtained on the person who contacted them.

Paragraph 3 Exemption from the secrecy requirement and absence of any liability whatsoever in case of reports made in good faith

133. The professional secrecy requirement ceases where the disclosure of information is authorised or required by legislation.

134. The law of 12 November 2004 as amended underlines that when a report is filed to the State prosecutor in good faith, the professionals of the financial sector incur no liability of any kind. In applying this notion which is wider than the mere reference to civil and criminal liability, the law also excludes any disciplinary liability.

135. It should also be stressed that the information on suspicions of money laundering or terrorist financing is communicated to the State prosecutor under the responsibility of the professional of the financial sector.

136. This exemption from liability does not cover disclosures in bad faith, such as notably disclosures of facts of which the professional of the financial sector is certain that they do not constitute evidence of money laundering or terrorist financing or disclosures made to prejudice the customer or the employer in the absence of the indications justifying such suspicion.

Paragraph 4 Obligation to transmit the same information to the CSSF as to the State prosecutor

137. The professionals of the financial sector shall transmit, separately and simultaneously, the same information to the CSSF as that transmitted to the State prosecutor under Article 5(1)(a) whatever the origin of the information process and the content of the information concerned, so that the CSSF may carry out its mission of prudential supervision.

Paragraph 5 Powers of the State prosecutor following the receipt of information

I. Instruction to block

138. Article 5(3) allows the State prosecutor to block one or several suspicious transaction(s), thereby confirming that the State prosecutor's block instruction may relate not only to a single transaction, but also to a set of operations relating to a suspicious transaction or to a customer suspected of intending to execute such transactions.

II. Time-restricted block instruction

139. Article 5(3) specifies the effect in time of a block instruction by the State prosecutor. An instruction of the State prosecutor to block the execution of one or several operations is valid for a maximum period of three months from the written or oral communication of the block instruction to the professional of the financial sector.
Where the instruction is communicated orally, it must be followed by a written confirmation from the State prosecutor within three days, otherwise the effects of the instruction cease on the third day at midnight.

Paragraph 6 Behaviour of the professional of the financial sector in the event of a suspicious transaction and information of the State prosecutor

I. Prohibition to execute the transaction before having informed the State prosecutor

140. The professionals of the financial sector are required to refrain from carrying out a transaction which they know or suspect to be related to money laundering or terrorist financing before having informed the State prosecutor thereof.
Where such transaction is suspected of giving rise to money laundering or terrorist financing operation and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the professionals of the financial sector concerned shall inform the State prosecutor immediately afterwards.

141. Professionals should nevertheless always avoid to execute a transaction if it is affected by measures to freeze without delay the funds or other assets of terrorist organisations or those who finance terrorism, notably in accordance with directly applicable national or EU measures.

II. Prohibition to tip off the customer whose transactions have been blocked or could be blocked owing to an investigation of the State prosecutor

142. Article 5(5) of the law of 12 November 2004 as amended clearly lays down the behaviour to adopt towards customers whose transactions have been blocked could be blocked as a result of a State prosecutor enquiry.

Principle and exception:

While Article 5(5) of the law of 12 November 2004 as amended confirms the general "*no tipping off*" principle, i.e. the ban on informing the customers or third parties concerned (the CSSF, the external auditors engaged to audit the accounts of the professionals of the financial sector and the lawyers advising the professionals of the financial sector are not considered third parties) that information has been transmitted to the State prosecutor or that an investigation into money laundering or terrorist financing is under way or could be started, Article 5(3) authorises the professional of the financial sector to refer to the State prosecutor's block instruction against the customer to justify its refusal to execute the customer order, where the customer requests such justification.

III. Relations with the group's internal control bodies

143. In order to coordinate the fight against money laundering and terrorist financing at the highest level of an international financial group to which the professional of the financial sector established in Luxembourg belongs, Luxembourg law allows to share information within the group in the following case.

144. Article 41 of the law of 5 April 1993 on the financial sector as amended, guarantees access, where necessary, for the internal control bodies of the group to which the professional of the financial sector established in Luxembourg belongs, to information concerning specific business relationships, in so far as this information is necessary to the

overall management of legal and reputational risks related to money laundering or terrorist financing under the Luxembourg law.
This exchange of information is not likely to contravene the "*no tipping off*" rule as it results from Article 5(5) of the law of 12 November 2004 as amended that the prohibition does not target this type of exchange of information.

Chapter 7 Requirements regarding bank and funds transfers

145. Pursuant to the second indent of Article 39 of the law of 5 April 1993 on the financial sector, as amended, credit institutions and other professionals of the financial sector (PFS) must abide by the rules set out in Regulation 1781/2006 of the European Parliament and the Council of 15 November 2006 on information on the payer accompanying transfers of funds as regards wire transfers (see Annexe IV). This provision which replaces the former second indent of Article 39 added by the law of 12 November 2004 confirms the application of the European regulation 1781/2006 which is in force since 1 January 2007 (see CSSF Circular 06/274 of 22 December 2006). It also transposes Article 15 of said European regulation which compels Member States to set out a sanctions regime by ensuring that the sanctions laid down in Article 63 of the law of 5 April 1993 on the financial sector, as amended, are applicable in this case.

Regulation (EC) 1781/2006 obliges the payment services provider of the payer to include information on the payer i.e. the customer on wire and funds transfers as well as on any associated messages. This information shall be more or less detailed depending on whether the wire transfers are carried out within the European Union or from the European Union to the outside. As far as the transfers within the European Union are concerned, instead of including the complete information as defined in the Regulation, a simplified regime can be applied according to which transfers need only include simplified information i.e. the account number of the payer or an identifier allowing the transaction to be traced back to the payer. In this case, the payment service provider of the payer shall nevertheless be able to make available to the payment service provider of the payee the complete information on the payer as laid down in Article 4 of the Regulation 1781/2006, within three working days of receiving the request of the payee. It is thus also possible to apply the regime requiring full information to transfers of funds within the European Union.

Regulation (EC) 1781/2006 also imposes duties on the payment service provider of the payee relating in particular to the detection of transfers on which information regarding the payer is missing.

In order to assess whether the required information on the payer is actually on the transfer of funds and to facilitate the detection of suspicious operations, the relevant professionals need to set up efficient procedures to detect missing information on the payer.

In this context, the paper on the "*Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying fund transfers to payment service providers of payees "* drawn up by CEBS, CESR and CEIOPS

provides information set to help the professionals in question to comply with the provisions of the relevant European regulation (Annexe V).

Title 3 Control of compliance with professional obligations

Chapter 1 The competent authority: the CSSF

146. Article 15 of the law of 12 November 2004 as amended provides that the CSSF is the competent authority to ensure compliance with professional obligations with regard to the fight against money laundering and terrorist financing without prejudice to the competence of the State prosecutor, and thereby expressly confirms the role played by the CSSF in the field of anti-money laundering and terrorist financing.

147. To fulfil this mission, the CSSF:

- carries out on-site inspections on a regular basis;

- requires, in the event of a report to the State prosecutor, that a copy of the relevant file is transmitted at the same time to the CSSF. The files shall also be transmitted to the CSSF where the investigation has been initiated by the competent judicial authorities;

- requires, on the one hand, that the mandate that the professionals of the financial sector award their external auditors for the audit of the annual accounts includes the review of compliance with legal provisions as regards the fight against money laundering and terrorist financing, the CSSF circulars in this respect, as well as the proper implementation of the relevant internal procedures and, on the other hand, that the report of the external auditor is transmitted to the CSSF;

- requires that compliance with these obligations and procedures is reviewed on a frequent basis by the compliance officer of the professional of the financial sector and by its internal audit department.

Chapter 2 The external auditor

148. The mandate that professionals of the financial sector award their external auditor for the audit of the annual accounts shall include the review of compliance with the legal professional obligations with regard to combating money laundering and terrorist financing, of this and other circulars, as well as the proper implementation of the relevant internal anti-money laundering and terrorist financing procedures.

149. The long-form report shall describe the anti-money laundering and terrorist financing procedures set up by the institution, as laid down in the law of 12 November 2004 as amended, in Article 39 of the law of 5 April 1993 as amended, as well as in this Circular.

The long-form report shall provide, in particular:
- a description of the customer acceptance policy;

- an appraisal of the adequacy of the internal procedures of the professional of the financial sector with regard to combating money laundering and terrorist financing and their compliance with the provisions of the law of 12 November 2004 as amended, of Article 39 of the law of 5 April 1993 as amended, as well as of this Circular, notably as regards identification of customers and beneficial owners. The external auditor shall also review the proper implementation of the procedures concerned. The outcome of these controls shall be presented in the annexe in the summary schedule "Compliance with this Circular" of IRE (*Institut des réviseurs d'entreprises*, Luxembourg Institute of auditors). This IRE schedule, which shall be completed with the comments "yes", "no" and "n/a" (not applicable), shall be completed, where applicable, by figures or supplementary explanations. The auditor may also refer to the outcome of these controls in other sections of the long-form report;
- a statement on the regular performance of such controls of compliance with procedures by the internal audit department and the compliance officer;
- employee training and information on the detection of money laundering and terrorist financing operations;
- historical statistics concerning the detected suspicious transactions, the number of suspicious transaction cases reported to the State prosecutor by the professional of the financial sector, as well as the total amount of funds involved.

The external auditor shall state how the sample of reviewed files was selected, as well as the coverage ratio of the population (number of files reviewed / total number of customers; volume of deposits reviewed / total volume of deposits).

150. Where the external auditor identifies cases of non-compliance with the legal or regulatory provisions or deficiencies, the external auditor shall give detailed indications enabling the CSSF to assess the situation (number of incomplete and pending files as well as with respect to the total number of reviewed files, details of the deficiencies identified, etc.).
It should be noted that external auditors shall also inform the CSSF of all the declarations made under Article 9-1 of the law of 28 June 1984 on the organisation of the auditing profession as amended, which relate to a professional of the financial sector under the supervision of the CSSF.

151. Luxembourg branches of EU credit institutions and investment firms shall, pursuant to the law of 5 April 1993 as amended, appoint an external auditor to perform the necessary controls in the Luxembourg branch in accordance with the Luxembourg standards. The branch shall communicate the audit report issued by the external auditor to the CSSF.

Chapter 3 The internal auditor and the anti-money laundering and terrorist financing officer

152. Compliance with the legal and regulatory provisions, as well as with the procedures relating to the fight against money laundering and terrorist financing shall be verified very frequently by the anti-money laundering and terrorist financing officer. These controls shall be coordinated with the controls the internal audit department is required to carry out in this area.

Moreover, professionals of the financial sector shall define their programmes and terms according to which these checks should be performed.

Title 4 Criminal and administrative sanctions in the event of non-compliance with professional obligations

153. Non-compliance with any professional obligations, excluding those concerning bank transfers, committed knowingly is liable to a fine of between EUR 1,250 to EUR 125,000. Such penal sanctions apply even in the absence of a money-laundering or terrorist financing offence.
Infringements to professional obligations are also liable to an administrative fine pursuant to Article 63 of the law of 5 April 1993 on the financial sector, as amended.

Non-respect of the provisions of Regulation (EC) 1781/2006 referred to in Article 39 of the law of 5 April 1993 on the financial sector, as amended is also punishable by an administrative fine laid down in Article 63 of the law of 5 April 1993 on the financial sector, as amended.

Part III Repealing provisions

154. This Circular replaces Circular CSSF 05/211 of 13 October 2005.

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Simone DELCOURT Director	Jean-Nicolas SCHAUS Director General

Annexes.

ANNEX I

Grand – Ducal Regulation of 29 July 2008 establishing the list of "third countries which impose equivalent requirements" within the meaning of the law of 12 November 2004 on the fight against money laundering and terrorist financing as amended. (Mémorial A n° 119 of 11.08.2008 p 1811).

[ ]

Art. 1 The list of "third countries which impose equivalent requirements" within the meaning of the law of 12 November 2004 on the fight against money laundering and terrorist financing as amended, is as follows:

- South Africa,
- Argentina,
- Australia,
- Brazil,
- Canada,
- United States,
- Guernsey,
- Hong Kong,
- Isle of Man,
- Japan,
- Jersey,
- Mexico,
- New Zealand,
- Russian Federation,
- Singapore,
- Switzerland,
- French overseas territories: Mayotte Island, New Caledonia, French Polynesia, St Pierre and Miquelon, Wallis and Futuna,
- Dutch overseas territories: Dutch West Indies, Aruba.

Art. 2. Our Minister for the Treasury and Budget shall execute this regulation, which shall be published in the Mémorial.

[ ]

ANNEX II

Money laundering indicators

The following list, adapted from a list drawn up by the Swiss Federal Banking Commission, primarily intends to raise awareness among the staff of banks and other professionals of the financial sector and claims in no way to be comprehensive. A comprehensive list would require constant updating to take into account new money-laundering methods. A single indicator or a suspicious transaction is not necessarily in itself sufficient grounds for suspecting a money-laundering operation.

In practice, only the combination of several indicators or suspicious transactions may be indicative of a money-laundering activity.

I. General indicators

Particular money-laundering risks are inherent in transactions:

- where the structure indicates an illegal purpose, where the economic purpose is unclear, or where the transactions appear absurd from an economic point of view;

- where assets are withdrawn shortly after having been deposited on an account (pass-through account), provided that the customer's activity does not furnish a plausible reason for this immediate withdrawal;

- where the customer's reasons for selecting this particular bank or branch for his business are unclear;

- where, as a result, an account which was previously mostly dormant becomes extremely active without plausible reason;

- that are inconsistent with the financial intermediary's knowledge and experience of the customer or the stated purpose of the business relationship.

Moreover, customers who provide false or misleading information to the financial intermediary or refuse without plausible explanation to provide the necessary information and documentation routinely required for the relevant business activity, must be treated with suspicion.

There may be grounds for suspicion if a customer regularly receives transfers from a bank established in a country considered non-cooperative by the Financial Action Task Force (FATF), or if a customer regularly performs transfers to such a country.

II. Specific indicators

1. Cash transactions

- Exchange of a large amount of small-denomination banknotes (euros or foreign currency) for large-denomination banknotes.

- Major currency exchange without entry in the customer's account.

- Cashing of cheques, including travellers' cheques for large amounts.

- Purchase or sale of large amounts of precious metals by occasional customers.

- Purchase of bank drafts for a large amount by occasional customers.

- Transfer orders abroad performed by occasional customers, without apparent legitimate reason.

- Frequent cash transactions in amounts just below the threshold above which customer identification is required.

- Acquisition of bearer securities with physical delivery.

2. Account and deposit transations

- Frequent withdrawals of cash, not justified by the customer's activity.

- Use of international trade financing methods, even though the use of such instruments is inconsistent with the stated activity of the customer.

- Accounts used intensively for payments, even though the accounts usually receive no or few payments.

- Absurd economic structure of the business relationship between the customer and the bank (large number of accounts with the same institution, frequent transfers between accounts, excessive liquidity, etc.).

- Provision of security (pledges, guarantees, etc.) by third parties unknown to the bank who do not seem to be closely related to the customer nor to have a plausible reason for granting such guarantees.

- Transfers to another bank without indication of the beneficiary.

- Acceptance of transfers from other banks without indication of the name or account number of he benficiary or the transferor.

- Repeated large amount transfers abroad with instruction to pay the beneficiary in cash.

- Large and repeated transfers to or from drug-producing countries.

- Provision of deposits or bank guarantees to secure loans between third parties, which are not in conformity with market terms.

- Cash payments by a large number of different individuals into a single account.

- Unexpected repayment of a non-performing loan, without reasonable explanation.

- Use of pseudonym or electronic accounts for commercial transactions by tradesmen, commercial or industrial companies.

- Withdrawal of assets shortly after having been deposited on an account (pass-through account).

3. Fiduciary transactions

- Fiduciary loans (back-to-back loans) without obvious legal reason.

- Holding of shares in a fiduciary capacity in non-listed companies, whose activity the bank is unable to determine.

4. Others

- Attempts of the customer to avoid personal contact with the professional of the financial sector.

III. Qualified indicators

- Customer requesting to close an account and to open new accounts in his/her name or in the name of certain members of his/her family without leaving a paper trail at the bank.

- Customer requesting to obtain receipt for cash withdrawals or deliveries of securities which where not effectively performed or which have been immediately deposited afterwards in the same institution.

- Customer requesting the execution of payment orders incorrectly indicating the remitter.

- Customer requesting that certain payments be performed through a nostro account of the professional of the financial sector or a "sundry" account, instead of his own account.

- Customer requesting to accept or document guarantees that are inconsistent with the economic reality or to grant back-to-back loans based on fictitious coverage.

- Criminal proceedings against a customer of the professional of the financial sector for crime, corruption or misuse of public funds.

Annexe III

Circulars concerning

- identification and declaration of business relationships with terrorist circles in accordance with EC Council Regulations imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban;
- combating money laundering

An updated list of these circulars is available on the CSSF website (www.cssf.lu).

Useful website as regards terrorist lists:

http://ec.europa.eu/external_relations/cfsp/sanctions/index.htm

ANNEX IV

Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 relating to the information on the payer accompanying transfers of funds

I

(Acts whose publication is obligatory)

REGULATION (EC) No 1781/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 15 November 2006

on information on the payer accompanying transfers of funds

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Central Bank [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Flows of dirty money through transfers of funds can damage the stability and reputation of the financial sector and threaten the internal market. Terrorism shakes the very foundations of our society. The soundness, integrity and stability of the system of transfers of funds and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to transfer funds for terrorist purposes.

(2) In order to facilitate their criminal activities, money launderers and terrorist financers could try to take advantage of the freedom of capital movements entailed by the integrated financial area, unless certain coordinating measures are adopted at Community level. By its scale, Community action should ensure that Special Recommendation VII on wire transfers (SR VII) of the Financial Action Task Force (FATF) established by the Paris G7 Summit of 1989 is transposed uniformly throughout the European Union, and, in particular, that there is no discrimination between national payments within a Member State and cross-border payments between Member States. Uncoordinated action by Member States alone in the field of cross-border transfers of funds could have a significant impact on the smooth functioning of payment systems at EU level, and therefore damage the internal market in the field of financial services.

(3) In the wake of the terrorist attacks in the USA on 11 September 2001, the extraordinary European Council on 21 September 2001 reiterated that the fight against terrorism is a key objective of the European Union. The European Council approved a plan of action dealing with enhanced police and judicial cooperation, developing international legal instruments against terrorism, preventing terrorist funding, strengthening air security and greater consistency between all relevant policies. This plan of action was revised by the European Council following the terrorist attacks of 11 March 2004 in Madrid, and now specifically addresses the need to ensure that the legislative framework created by the Community for the purpose of combating terrorism and improving judicial cooperation is adapted to the nine Special Recommendations against Terrorist Financing adopted by the FATF.

(4) In order to prevent terrorist funding, measures aimed at the freezing of funds and economic resources of certain persons, groups and entities have been taken, including Regulation (EC) No 2580/2001 [3], and Council Regulation (EC) No 881/2002 [4]. To that same end, measures aimed at protecting the financial system against the channelling of funds and economic resources for terrorist purposes have been taken. Directive 2005/60/EC of the European Parliament and of the Council [5] contains a number of measures aimed at combating the misuse of the financial system for the purpose of money laundering and terrorist financing. Those measures do not, however, fully prevent terrorists and other criminals from having access to payment systems for moving their funds.

---

[1] OJ C 336, 31.12.2005, p. 109.

[2] Opinion of the European Parliament delivered on 6 July 2006 (not yet published in the Official Journal) and Council Decision delivered on 7 November 2006.

[3] OJ L 344, 28.12.2001, p. 70. Regulation as last amended by Commission Regulation (EC) No 1461/2006 (OJ L 272, 3.10.2006, p. 11).

[4] OJ L 139, 29.5.2002, p. 9. Regulation as last amended by Commission Regulation (EC) No 1508/2006 (OJ L 280, 12.10.2006, p. 12).

[5] OJ L 309, 25.11.2005, p. 15.

(5) In order to foster a coherent approach in the international context in the field of combating money laundering and terrorist financing, further Community action should take account of developments at that level, namely the nine Special Recommendations against Terrorist Financing adopted by the FATF, and in particular SR VII and the revised interpretative note for its implementation.

(6) The full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, investigation and detection of money laundering or terrorist financing. It is therefore appropriate, in order to ensure the transmission of information on the payer throughout the payment chain, to provide for a system imposing the obligation on payment service providers to have transfers of funds accompanied by accurate and meaningful information on the payer.

(7) The provisions of this Regulation apply without prejudice to Directive 95/46/EC of the European Parliament and of the Council [1]. For example, information collected and kept for the purpose of this Regulation should not be used for commercial purposes.

(8) Persons who merely convert paper documents into electronic data and are acting under a contract with a payment service provider do not fall within the scope of this Regulation; the same applies to any natural or legal person who provides payment service providers solely with messaging or other support systems for transmitting funds or with clearing and settlement systems.

(9) It is appropriate to exclude from the scope of this Regulation transfers of funds that represent a low risk of money laundering or terrorist financing. Such exclusions should cover credit or debit cards, Automated Teller Machine (ATM) withdrawals, direct debits, truncated cheques, payments of taxes, fines or other levies, and transfers of funds where both the payer and the payee are payment service providers acting on their own behalf. In addition, in order to reflect the special characteristics of national payment systems, Member States may exempt electronic giro payments, provided that it is always possible to trace the transfer of funds back to the payer. Where Member States have applied the derogation for electronic money in Directive 2005/60/EC, it should be applied under this Regulation, provided the amount transacted does not exceed EUR 1 000.

(10) The exemption for electronic money, as defined by Directive 2000/46/EC of the European Parliament and of the Council [2], covers electronic money irrespective of whether the issuer of such money benefits from a waiver under Article 8 of that Directive.

(11) In order not to impair the efficiency of payment systems, the verification requirements for transfers of funds made from an account should be separate from those for transfers of funds not made from an account. In order to balance the risk of driving transactions underground by imposing overly strict identification requirements against the potential terrorist threat posed by small transfers of funds, the obligation to check whether the information on the payer is accurate should, in the case of transfers of funds not made from an account, be imposed only in respect of individual transfers of funds that exceed EUR 1 000, without prejudice to the obligations under Directive 2005/60/EC. For transfers of funds made from an account, payment service providers should not be required to verify information on the payer accompanying each transfer of funds, where the obligations under Directive 2005/60/EC have been met.

(12) Against the background of Regulation (EC) No 2560/2001 of the European Parliament and of the Council [3] and the Commission Communication 'A New Legal Framework for Payments in the Internal Market', it is sufficient to provide for simplified information on the payer to accompany transfers of funds within the Community.

(13) In order to allow the authorities responsible for combating money laundering or terrorist financing in third countries to trace the source of funds used for those purposes, transfers of funds from the Community to outside the Community should carry complete information on the payer. Those authorities should be granted access to complete information on the payer only for the purposes of preventing, investigating and detecting money laundering or terrorist financing.

(14) For transfers of funds from a single payer to several payees to be sent in an inexpensive way in batch files containing individual transfers from the Community to outside the Community, provision should be made for such individual transfers to carry only the account number of the payer or a unique identifier provided that the batch file contains complete information on the payer.

(15) In order to check whether the required information on the payer accompanies transfers of funds, and to help to identify suspicious transactions, the payment service provider of the payee should have effective procedures in place in order to detect whether information on the payer is missing.

[1] OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

[2] OJ L 275, 27.10.2000, p. 39.

[3] Regulation as corrected by OJ L 344, 28.12.2001, p. 13.

(16) Owing to the potential terrorist financing threat posed by anonymous transfers, it is appropriate to enable the payment service provider of the payee to avoid or correct such situations when it becomes aware that information on the payer is missing or incomplete. In this regard, flexibility should be allowed as concerns the extent of information on the payer on a risk-sensitive basis. In addition, the accuracy and completeness of information on the payer should remain the responsibility of the payment service provider of the payer. Where the payment service provider of the payer is situated outside the territory of the Community, enhanced customer due diligence should be applied, in accordance with Directive 2005/60/EC, in respect of cross-border correspondent banking relationships with that payment service provider.

(17) Where guidance is given by national competent authorities as regards the obligations either to reject all transfers from a payment service provider which regularly fails to supply the required information on the payer or to decide whether or not to restrict or terminate a business relationship with that payment service provider, it should inter alia be based on the convergence of best practices and should also take into account the fact that the revised interpretative note to SR VII of the FATF allows third countries to set a threshold of EUR 1 000 or USD 1 000 for the obligation to send information on the payer, without prejudice to the objective of efficiently combating money laundering and terrorist financing.

(18) In any event, the payment service provider of the payee should exercise special vigilance, assessing the risks, when it becomes aware that information on the payer is missing or incomplete, and should report suspicious transactions to the competent authorities, in accordance with the reporting obligations set out in Directive 2005/60/EC and national implementing measures.

(19) The provisions on transfers of funds where information on the payer is missing or incomplete apply without prejudice to any obligations on payment service providers to suspend and/or reject transfers of funds which violate provisions of civil, administrative or criminal law.

(20) Until technical limitations that may prevent intermediary payment service providers from satisfying the obligation to transmit all the information they receive on the payer are removed, those intermediary payment service providers should keep records of that information. Such technical limitations should be removed as soon as payment systems are upgraded.

(21) Since in criminal investigations it may not be possible to identify the data required or the individuals involved until many months, or even years, after the original transfer of funds, it is appropriate to require payment service providers to keep records of information on the payer for the purposes of preventing, investigating and detecting money laundering or terrorist financing. This period should be limited.

(22) To enable prompt action to be taken in the fight against terrorism, payment service providers should respond promptly to requests for information on the payer from the authorities responsible for combating money laundering or terrorist financing in the Member State where they are situated.

(23) The number of working days in the Member State of the payment service provider of the payer determines the number of days to respond to requests for information on the payer.

(24) Given the importance of the fight against money laundering and terrorist financing, Member States should lay down effective, proportionate and dissuasive penalties in national law for failure to comply with this Regulation.

(25) The measures necessary for the implementation of this Regulation should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission [1].

(26) A number of countries and territories which do not form part of the territory of the Community share a monetary union with a Member State, form part of the currency area of a Member State or have signed a monetary convention with the European Community represented by a Member State, and have payment service providers that participate directly or indirectly in the payment and settlement systems of that Member State. In order to avoid the application of this Regulation to transfers of funds between the Member States concerned and those countries or territories having a significant negative effect on the economies of those countries or territories, it is appropriate to provide for the possibility for such transfers of funds to be treated as transfers of funds within the Member States concerned.

[1] OJ L 184, 17.7.1999, p. 23. Decision as last amended by Decision 2006/512/EC (OJ L 200, 22.7.2006, p. 11).

(27) In order not to discourage donations for charitable purposes, it is appropriate to authorise Member States to exempt payment services providers situated in their territory from collecting, verifying, recording, or sending information on the payer for transfers of funds up to a maximum amount of EUR 150 executed within the territory of that Member State. It is also appropriate to make this option conditional upon requirements to be met by non-profit organisations, in order to allow Member States to ensure that this exemption does not give rise to abuse by terrorists as a cover for or a means of facilitating the financing of their activities.

(28) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(29) In order to establish a coherent approach in the field of combating money laundering and terrorist financing, the main provisions of this Regulation should apply from the same date as the relevant provisions adopted at international level,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

SUBJECT MATTER, DEFINITIONS AND SCOPE

Article 1

Subject matter

This Regulation lays down rules on information on the payer to accompany transfers of funds for the purposes of the prevention, investigation and detection of money laundering and terrorist financing.

Article 2

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) 'terrorist financing' means the provision or collection of funds within the meaning of Article 1(4) of Directive 2005/60/EC;

(2) 'money laundering' means any conduct which, when committed intentionally, is regarded as money laundering for the purposes of Article 1(2) or (3) of Directive 2005/60/EC;

(3) 'payer' means either a natural or legal person who holds an account and allows a transfer of funds from that account, or, where there is no account, a natural or legal person who places an order for a transfer of funds;

(4) 'payee' means a natural or legal person who is the intended final recipient of transferred funds;

(5) 'payment service provider' means a natural or legal person whose business includes the provision of transfer of funds services;

(6) 'intermediary payment service provider' means a payment service provider, neither of the payer nor of the payee, that participates in the execution of transfers of funds;

(7) 'transfer of funds' means any transaction carried out on behalf of a payer through a payment service provider by electronic means, with a view to making funds available to a payee at a payment service provider, irrespective of whether the payer and the payee are the same person;

(8) 'batch file transfer' means several individual transfers of funds which are bundled together for transmission;

(9) 'unique identifier' means a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used to effect the transfer of funds.

Article 3

Scope

1. This Regulation shall apply to transfers of funds, in any currency, which are sent or received by a payment service provider established in the Community.

2. This Regulation shall not apply to transfers of funds carried out using a credit or debit card, provided that:

(a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services;

and

(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies such transfer of funds.

3. Where a Member State chooses to apply the derogation set out in Article 11(5)(d) of Directive 2005/60/EC, this Regulation shall not apply to transfers of funds using electronic money covered by that derogation, except where the amount transferred exceeds EUR 1 000.

4. Without prejudice to paragraph 3, this Regulation shall not apply to transfers of funds carried out by means of a mobile telephone or any other digital or Information Technology (IT) device, when such transfers are pre-paid and do not exceed EUR 150.

5. This Regulation shall not apply to transfers of funds carried out by means of a mobile telephone or any other digital or IT device, when such transfers are post-paid and meet all of the following conditions:

(a) the payee has an agreement with the payment service provider permitting payment for the provision of goods and services;

(b) a unique identifier, allowing the transaction to be traced back to the payer, accompanies the transfer of funds;

and

(c) the payment service provider is subject to the obligations set out in Directive 2005/60/EC.

6. Member States may decide not to apply this Regulation to transfers of funds within that Member State to a payee account permitting payment for the provision of goods or services if:

(a) the payment service provider of the payee is subject to the obligations set out in Directive 2005/60/EC;

(b) the payment service provider of the payee is able by means of a unique reference number to trace back, through the payee, the transfer of funds from the natural or legal person who has an agreement with the payee for the provision of goods and services;

and

(c) the amount transacted is EUR 1 000 or less.

Member States making use of this derogation shall inform the Commission thereof.

7. This Regulation shall not apply to transfers of funds:

(a) where the payer withdraws cash from his or her own account;

(b) where there is a debit transfer authorisation between two parties permitting payments between them through accounts, provided that a unique identifier accompanies the transfer of funds, enabling the natural or legal person to be traced back;

(c) where truncated cheques are used;

(d) to public authorities for taxes, fines or other levies within a Member State;

(e) where both the payer and the payee are payment service providers acting on their own behalf.

CHAPTER II

OBLIGATIONS ON THE PAYMENT SERVICE PROVIDER OF THE PAYER

Article 4

Complete information on the payer

1. Complete information on the payer shall consist of his name, address and account number.

2. The address may be substituted with the date and place of birth of the payer, his customer identification number or national identity number.

3. Where the payer does not have an account number, the payment service provider of the payer shall substitute it by a unique identifier which allows the transaction to be traced back to the payer.

Article 5

Information accompanying transfers of funds and record keeping

1. Payment service providers shall ensure that transfers of funds are accompanied by complete information on the payer.

2. The payment service provider of the payer shall, before transferring the funds, verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source.

3. In the case of transfers of funds from an account, verification may be deemed to have taken place if:

(a) a payer's identity has been verified in connection with the opening of the account and the information obtained by this verification has been stored in accordance with the obligations set out in Articles 8(2) and 30(a) of Directive 2005/60/EC;

or

(b) the payer falls within the scope of Article 9(6) of Directive 2005/60/EC.

4. However, without prejudice to Article 7(c) of Directive 2005/60/EC, in the case of transfers of funds not made from an account, the payment service provider of the payer shall verify the information on the payer only where the amount exceeds EUR 1 000, unless the transaction is carried out in several operations that appear to be linked and together exceed EUR 1 000.

5. The payment service provider of the payer shall for five years keep records of complete information on the payer which accompanies transfers of funds.

Article 6

Transfers of funds within the Community

1. By way of derogation from Article 5(1), where both the payment service provider of the payer and the payment service provider of the payee are situated in the Community, transfers of funds shall be required to be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer.

2. However, if so requested by the payment service provider of the payee, the payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer, within three working days of receiving that request.

Article 7

Transfers of funds from the Community to outside the Community

1. Transfers of funds where the payment service provider of the payee is situated outside the Community shall be accompanied by complete information on the payer.

2. In the case of batch file transfers from a single payer where the payment service providers of the payees are situated outside the Community, paragraph 1 shall not apply to the individual transfers bundled together therein, provided that the batch file contains that information and that the individual transfers carry the account number of the payer or a unique identifier.

CHAPTER III

OBLIGATIONS ON THE PAYMENT SERVICE PROVIDER OF THE PAYEE

Article 8

Detection of missing information on the payer

The payment service provider of the payee shall detect whether, in the messaging or payment and settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system. Such provider shall have effective procedures in place in order to detect whether the following information on the payer is missing:

(a) for transfers of funds where the payment service provider of the payer is situated in the Community, the information required under Article 6;

(b) for transfers of funds where the payment service provider of the payer is situated outside the Community, complete information on the payer as referred to in Article 4, or where applicable, the information required under Article 13;

and

(c) for batch file transfers where the payment service provider of the payer is situated outside the Community, complete information on the payer as referred to in Article 4 in the batch file transfer only, but not in the individual transfers bundled therein.

Article 9

Transfers of funds with missing or incomplete information on the payer

1. If the payment service provider of the payee becomes aware, when receiving transfers of funds, that information on the payer required under this Regulation is missing or incomplete, it shall either reject the transfer or ask for complete information on the payer. In any event, the payment service provider of the payee shall comply with any applicable law or administrative provisions relating to money laundering and terrorist financing, in particular, Regulations (EC) No 2580/2001 and (EC) No 881/2002, Directive 2005/60/EC and any national implementing measures.

2. Where a payment service provider regularly fails to supply the required information on the payer, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider or deciding whether or not to restrict or terminate its business relationship with that payment service provider.

The payment service provider of the payee shall report that fact to the authorities responsible for combating money laundering or terrorist financing.

Article 10

Risk-based assessment

The payment service provider of the payee shall consider missing or incomplete information on the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported, in accordance with the obligations set out in Chapter III of Directive 2005/60/EC, to the authorities responsible for combating money laundering or terrorist financing.

Article 11

Record keeping

The payment service provider of the payee shall for five years keep records of any information received on the payer.

CHAPTER IV

OBLIGATIONS ON INTERMEDIARY PAYMENT SERVICE PROVIDERS

Article 12

Keeping information on the payer with the transfer

Intermediary payment service providers shall ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer.

Article 13

Technical limitations

1. This Article shall apply where the payment service provider of the payer is situated outside the Community and the intermediary payment service provider is situated within the Community.

2. Unless the intermediary payment service provider becomes aware, when receiving a transfer of funds, that information on the payer required under this Regulation is missing or incomplete, it may use a payment system with technical limitations which prevents information on the payer from accompanying the transfer of funds to send transfers of funds to the payment service provider of the payee.

3. Where the intermediary payment service provider becomes aware, when receiving a transfer of funds, that information on the payer required under this Regulation is missing or incomplete, it shall only use a payment system with technical limitations if it is able to inform the payment service provider of the payee thereof, either within a messaging or payment system that provides for communication of this fact or through another procedure, provided that the manner of communication is accepted by, or agreed between, both payment service providers.

4. Where the intermediary payment service provider uses a payment system with technical limitations, the intermediary payment service provider shall, upon request from the payment service provider of the payee, make available to that payment service provider all the information on the payer which it has received, irrespective of whether it is complete or not, within three working days of receiving that request.

5. In the cases referred to in paragraphs 2 and 3, the intermediary payment service provider shall for five years keep records of all information received.

CHAPTER V

GENERAL OBLIGATIONS AND IMPLEMENTING POWERS

Article 14

Cooperation obligations

Payment service providers shall respond fully and without delay, in accordance with the procedural requirements established in the national law of the Member State in which they are situated, to enquiries from the authorities responsible for combating money laundering or terrorist financing of that Member State concerning the information on the payer accompanying transfers of funds and corresponding records.

Without prejudice to national criminal law and the protection of fundamental rights, those authorities may use that information only for the purposes of preventing, investigating or detecting money laundering or terrorist financing.

Article 15

Penalties and monitoring

1. Member States shall lay down the rules on penalties applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive. They shall apply from 15 December 2007.

2. Member States shall notify the Commission of the rules referred to in paragraph 1 and the authorities responsible for their application by 14 December 2007at the latest, and shall notify it without delay of any subsequent amendment affecting them.

3. Member States shall require competent authorities to effectively monitor, and take necessary measures with a view to ensuring, compliance with the requirements of this Regulation.

Article 16

Committee procedure

1. The Commission shall be assisted by the Committee on the Prevention of Money Laundering and Terrorist Financing established by Directive 2005/60/EC, hereinafter referred to as 'the Committee'.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof and provided that the implementing measures adopted in accordance with this procedure do not modify the essential provisions of this Regulation.

The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.

CHAPTER VI

DEROGATIONS

Article 17

Agreements with territories or countries which do not form part of the territory of the Community

1. The Commission may authorise any Member State to conclude agreements, under national arrangements, with a country or territory which does not form part of the territory of the Community as determined in accordance with Article 299 of the Treaty, which contain derogations from this Regulation, in order to allow for transfers of funds between that country or territory and the Member State concerned to be treated as transfers of funds within that Member State.

Such agreements may be authorised only if:

(a) the country or territory concerned shares a monetary union with the Member State concerned, forms part of the currency area of that Member State or has signed a Monetary Convention with the European Community represented by a Member State;

(b) payment service providers in the country or territory concerned participate directly or indirectly in payment and settlement systems in that Member State;

and

(c) the country or territory concerned requires payment service providers under its jurisdiction to apply the same rules as those established under this Regulation.

2. Any Member State wishing to conclude an agreement as referred to in paragraph 1 shall send an application to the Commission and provide it with all the necessary information.

Upon receipt by the Commission of an application from a Member State, transfers of funds between that Member State and the country or territory concerned shall be provisionally treated as transfers of funds within that Member State, until a decision is reached in accordance with the procedure set out in this Article.

If the Commission considers that it does not have all the necessary information, it shall contact the Member State concerned within two months of receipt of the application and specify the additional information required.

Once the Commission has all the information it considers necessary for appraisal of the request, it shall within one month notify the requesting Member State accordingly and shall transmit the request to the other Member States.

3. Within three months of the notification referred to in the fourth subparagraph of paragraph 2, the Commission shall decide, in accordance with the procedure referred to in Article 16(2), whether to authorise the Member State concerned to conclude the agreement referred to in paragraph 1 of this Article.

In any event, a decision as referred to in the first subparagraph shall be adopted within eighteen months of receipt of the application by the Commission.

Article 18

Transfers of funds to non-profit organisations within a Member State

1. Member States may exempt payment service providers situated in their territory from the obligations set out in Article 5, as regards transfers of funds to organisations carrying out activities for non-profit charitable, religious, cultural, educational, social, scientific or fraternal purposes, provided that those organisations are subject to reporting and external audit requirements or supervision by a public authority or self-regulatory body recognised under national law and that those transfers of funds are limited to a maximum amount of EUR 150 per transfer and take place exclusively within the territory of that Member State.

2. Member States making use of this Article shall communicate to the Commission the measures that they have adopted for applying the option provided for in paragraph 1, including a list of organisations covered by the exemption, the names of the natural persons who ultimately control those organisations and an explanation of how the list will be updated. That information shall also be made available to the authorities responsible for combating money laundering and terrorist financing.

3. An up-to-date list of organisations covered by the exemption shall be communicated by the Member State concerned to the payment service providers operating in that Member State.

Article 19

Review clause

1. By 28 December 2011 the Commission shall present a report to the European Parliament and to the Council giving a full economic and legal assessment of the application of this Regulation, accompanied, if appropriate, by a proposal for its modification or repeal.

2. That report shall in particular review:

(a) the application of Article 3 with regard to further experience of the possible misuse of electronic money, as defined in Article 1(3) of Directive 2000/46/EC, and other newly-developed means of payment, for the purposes of money laundering and terrorist financing. Should there be a risk of such misuse, the Commission shall submit a proposal to amend this Regulation;

(b) the application of Article 13 with regard to the technical limitations which may prevent complete information on the payer from being transmitted to the payment service provider of the payee. Should it be possible to overcome such technical limitations in the light of new developments in the payments area, and taking into account related costs for payment service providers, the Commission shall submit a proposal to amend this Regulation.

CHAPTER VII

FINAL PROVISIONS

Article 20

Entry into force

This Regulation shall enter into force on the 20th day following the day of its publication in the *Official Journal of the European Union*, but in any event not before 1 January 2007.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 15 November 2006.

For the European Parliament
The President
J. BORRELL FONTELLES

For the Council
The President
P. LEHTOMÄKI

ANNEX V

Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying fund transfers to payment service providers of payees

CEBS 2008 156 / CEIOPS-3L3-12-08 / CESR / 08-773

16 October 2008

Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees

Background

1. The European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees, which came into force on 1 January 2007, acts to implement the Financial Action Task Force's Special Recommendation VII in the European Union. The Regulation requires that Payment Service Providers "PSP"s (like banks and wire transfer offices) attach complete information about the payer to funds transfers made by electronic means. They must also check the information that accompanies incoming payments. The purpose of this regulation is to make it easier for the authorities to trace flows of money on occasions where that is deemed necessary.

2. This regulation sits alongside a wider body of EU and national legislation that aims to combat money laundering and the finance of terrorism, by, for example, mandating that financial institutions observe UN, EU and national sanctions, undertake due diligence checks on their customers when accounts are opened, monitor customers' behaviour on an ongoing basis, and inform the authorities when they form suspicions that they may have identified criminal or terrorist activity.

3. The Anti Money Laundering Task Force ("AMLTF") recognises that this Regulation is an important component of this wider regime. For example, when a bank checks incoming payments, it may find that information on the payer is missing or incomplete: this could be one of

the items of intelligence that contributes to a decision to file a suspicious transaction report with the authorities.

4. It has been brought to the AMLTF's attention that there appears to be an issue in relation to the information on the payer accompanying fund transfers to payment service providers of payees, arising out of this regulation. Further the Committee for the Prevention of Money Laundering and Terrorist Financing, chaired by the European Commission, and comprising of representatives from all Member States, asked the AMLTF to work on this topic, interacting with market participants. Also, the European Commission is ensuring appropriate contacts with the bodies working on payments issues too. The AMLTF has also analysed the possible conflict in the Regulation with the obligation to freeze the funds due to other provisions.

4. This paper aims to reflect a common understanding to deal with payments that lack the required information in respect of this regulation, which has been developed by the AMLTF, with the assistance of an informal consultation with the industry, including an Industry workshop held in January 2008, and has been subject to a three month public consultation launched in April 2008, which included a public hearing held on 6th May 2008.

5. This common understanding is based on the current functioning of payment, messaging and settlement systems, aims to ensure a level playing field between European payment service providers, and assist the reach of traceability[1] of transfers. This document aims to take into account the current level of compliance with the FATF Special Recommendation VII outside the EU, and the fact that funds transfers is a mass business. An annex describes some existing practices that our liaison with the financial services industry has identified. It outlines some measures that are currently being employed by payment services providers.

[1] Recital 6 of 1Directive 1781/2006 - The full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, investigation and detection of money laundering or terrorist financing. It is therefore appropriate, in order to ensure the transmission of information on the payer throughout the payment chain, to provide for a system imposing the obligation on payment service providers to have transfers of funds accompanied by accurate and meaningful information on the payer.

6. The AMLTF was established in the second half of 2006 by CEBS, CESR and CEIOPS (- the three Level Three Committees, 3L3), with a view to providing a supervisory contribution in anti-money laundering (AML) and Counter Terrorism Finance issues, with a specific focus on the Third Anti-Money Laundering Directive. The AMLTF is composed of competent authorities from across Europe with supervisory responsibility for payment service providers.
7. The AMLTF acknowledges that there will be other competent authorities with these responsibilities, who are not represented on its committee. The AMLTF suggest that this paper would nonetheless represent a useful resource to these authorities.

1. Introduction

1. This paper aims to reflect the common understanding of European supervisors concerning the application of Chapter III of the European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees (hereafter referred to as the "Regulation").

2. This common understanding is based on the current functioning of payment, messaging and settlement systems and aims to ensure a level playing field between European payment service providers (hereafter referred to as PSPs). The present common understanding takes into account the current level of compliance with the Special Recommendation VII outside the EU and the fact that funds transfers is a mass business.

3. This common understanding shall not be seen as an extension to this Regulation adding obligations, but rather as a clarification on the requirements in this Regulation, so as to provide PSPs with a common understanding of supervisory expectations on compliance with this Regulation.

2. Common understanding on Article 8 of the Regulation

4. PSPs shall have effective procedures in place in order to detect whether in the messaging, payment or settlement system used to effect a transfer of funds, the fields relating to the information on the payer are complete in accordance with Articles 4 and 6. It is expected that PSPs undertake this obligation by applying both of the following elements.

5. First, as stated by the Regulation, the PSP of the payee shall detect whether, in the messaging, payment or settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system.

6. This first element will generally result from the mere application of the validation rules of the messaging, payment or settlement system, if those validation rules prevent payments being sent or received where the mandatory information concerning the payer is not present at all.

7. However, it is recognised that it is very difficult for a standard filter to be able to assess the completeness of all messages and that there will be instances where the payer information fields are completed with incorrect /meaningless information, where the payment will pass through the system.

8. Further PSPs are encouraged to apply filters to detect obvious meaningless information, such as information clearly intended to circumvent the intention of FATF Special Recommendation VII and this Regulation, based on their own experience, so as to assist PSPs in assessing whether they have been provided with meaningful information, as if so, the PSPs will then be obliged to reject the transfer, or to ask for information. PSPs should endeavour to apply this first element at the time of the processing.

9. Second, unless the PSP has detected the incompleteness of all transfers at the time of processing, the PSP should in addition to Article 8.1, subject incoming payment traffic to an appropriate level of monitoring to detect incomplete transfers or those with meaningless information by proceeding to appropriate post event random sampling to detect non compliant payments. Such sampling could focus more heavily on transfers from those higher risk sending PSPs, notably those PSPs who are already been identified by such sampling as having previously failed to comply with the relevant information requirement. PSPs identified as regularly failing should receive a particular attention in the application of this post event random sampling.

3. Common understanding on Articles 9 §1 and 10 of the Regulation

10. By application of Article 8 along the lines suggested above, receiving PSPs may become aware of the incompleteness/meaninglessness of the information accompanying a transfer either at the time of processing (or even before), or later if undertaking the post event monitoring.

11. The present section takes into account Article 9 §1 and Article 10. The latter particularly refers to reporting obligations set out in Chapter III of the Third Directive. Chapter III of the Third Directive notably includes Articles 22 and 24 which are particularly important for the application of Article 9§1. Those Articles are taken into account by the present guidelines. It should also be noted that Article 9 §1 of the Regulation refers to Regulations 2580/2001 and 881/2002.

3.1 The PSP becomes aware, when receiving the transfer, that it is incomplete

12. If the PSP becomes aware on receipt of the transfer, that it is incomplete, it should either reject the transfer, or ask for complete information. While it is asking for the complete information, it may either execute the transfer or hold the funds by temporarily suspending the transfer (if holding the funds is allowed by national law, bearing in mind any legal and consumer obligations).

3.1.1 Internal policy, processes and procedures

13. PSPs should adopt a policy defining their reaction on becoming aware of an incomplete transfer or with meaningless information.

14. Except for those PSPs that choose to systematically reject all such transfers, the PSP should endeavour to apply a mix of point 3.1.3, with 3.1.4 and/or 3.1.2. Without prejudice to any other applicable law or Regulation if any, the PSP should normally not execute systematically all incomplete transfers or transfers with meaningless information.

15. The PSP should define the criteria on which internal processes and procedures will be based in order to distinguish between transfers that they will execute directly and those that they will hold and/or those that they will reject. The PSP should draft those internal processes and procedures taking into account all applicable obligations. They should particularly mitigate their compliance risk when holding the funds or rejecting the transfer. Furthermore, the PSP shall particularly comply with Regulations 2580/2001 and 881/2002 and with any other lists they have an obligation to apply as it is provided by their jurisdiction.

16. The policy, processes and procedures should be approved at an appropriate hierarchic level and should be reviewed regularly.

3.1.2 The PSP chooses to reject the transfer (if allowed by national law)

17. In this case, the PSP has no obligation to ask for the complete information. When rejecting a transfer, PSPs are encouraged to give the reason for the rejection to the PSP of the payer.

18. However, the PSP shall consider the incompleteness of the transfer or meaninglessness of the information as a factor in assessing whether any transaction related to the rejected transfer is suspicious and whether it must be reported to its FIU. The assessment of suspicion should be in accordance with existing Directives and requirements.

19. Depending on the risk criteria defined by the PSP in accordance with the risk based approach, the incompleteness/meaninglessness of information may or may not trigger the necessity to assess the transaction as being suspicious. If the transaction comes from a non EEA country which EU member states consider to be equivalent to the standards of the EU Directive 2005/60/EC, this could be considered accordingly in the risk assessment. PSPs should complete this assessment in accordance with the applicable obligations and their internal processes, procedures and policies.

3.1.3 The PSP chooses to execute the transfer

20. Knowing that the transfer is incomplete or has meaningless information, the PSP chooses to execute it before asking for the complete /meaningful information to the PSP of the payer.

21. After having executed the transfer, it has to ask for complete information.

Asking the complete information

22. In this regard, the PSP should define criteria that it will use in order to determine on which occurrence it will send the request for complete information to the PSP of the payer.

23. Further, a maximum deadline between the receipt of payment and issuing a request for complete/meaningful information should be set, such as 7 working days.

24. Once the PSP has sent its request for complete/meaningful information, it should set a reasonable timeframe, such as 7 working days, or longer for messages received from outside the EEA, to receive this information and then, if the level of risk requires it, assess the suspicious character of the transaction or any related transaction and, if it did not receive a satisfactory answer to its request for further information regarding the relevant transfer, proceed to follow up on its request.

Assessing the suspicious character

25. As mentioned under point 3.1.2, PSPs should complete this assessment in accordance with the applicable obligations and their internal processes, procedures and policies. Depending on the risk criteria defined by the PSP in accordance with the risk based approach, the risk factor resulting from the incompleteness /meaninglessness of information may or may not trigger an internal transmission to the AML/CFT officer for assessment of its suspicious character.

26. In addition, it should be kept in mind that recital 16 of the Regulation particularly states that the accuracy and completeness of information on the payer should remain the responsibility of the PSP of the payer. Therefore, the PSPs of payees cannot be held responsible for the lack of information accompanying transfers they receive, including if they execute *de bona fide* a transfer without complete information on the payer that they would not have executed if the complete information had been provided.

Follow up to the request for complete information.

27. The PSP has to define policies and set up procedures and processes in order to complete an appropriate follow up to its requests for complete /meaningful information. The PSP should be able to demonstrate to its supervisor that those policies, processes and procedures are adequate in order to fulfil their objectives, and are effective in their application. The PSP could keep a record of its request, including any lack of reply, and make such a record available to the authorities.

28. For example, if the PSP of the payee did not receive a satisfactory answer to its request for complete/meaningful information after expiry of its desired timeframe, it should send a reminder, again with a desired timeframe by when it would expect to receive a response, after the first deadline has run out. The PSP may chose to batch up its follow up requests to such non responding PSPs.

29. The reminder should also notify that the sending PSP, in case it will not answer satisfactory within the deadline, will in future be subject to the internal high risk monitoring (cf. above 2.2.) and treated under the conditions of Art. 9 (2) of Regulation 1781/2006. An alternative could be that the PSP may choose to state this in its Terms and Conditions.

3.1.4 The PSP chooses to hold the funds, (if allowed by national law)

30. Section 3.1.1 of this common understanding defines how a PSP has to proceed in order to determine its reaction towards an incomplete transfer or a transfer with meaningless information. As mentioned in that section, it should be stressed that a PSP can temporarily suspend the execution of the transfer and thus holds the funds if this is requested by, or compatible with, the legal or regulatory framework to which it is subject. However, apart from suspending the transfer on the basis of the option to ask for complete information defined by Regulation 1781/2006 it may be necessary to “freeze” the funds for an undefined period of time compliant

with relevant "freezing" measures and economic sanctions (like those set out in Regulations 2580/2001 and 881/2002), with the obligation to refrain from executing transactions which are reported as suspicious (article 24(1) of Directive 2005/60/EC) and with the order to postpone such transactions issued by the competent authority (article 24(1) of Directive 2005/60/EC).Further, it is also stressed that PSPs should particularly mitigate their legal and compliance risk when holding the funds or rejecting the transfer, including in relation to their contractual obligations.

31. It can be considered that it is particularly appropriate to apply this option when there is need for clearing the situation internally or with other group members, databases or the FIU[2] in order to establish or reject the suspicion of money laundering.

32. When the PSP chooses to hold the funds, its first action should be to ask for the complete /meaningful information.

Asking for the complete information

33. In this regard, the PSP should define criteria that it will use in order to determine on which occurrence it will send the request for complete /meaningful information to the PSP of the payer. However, those processes and procedures should ensure that the PSP will ask, ideally at least once every 7 working days (or longer for payments from outside the EEA), for the complete /meaningful information from each PSP that sent at least one incomplete transfer during the previous 7 working days. The attention of the PSP is drawn on the fact that even if the maximum allowed deadline is the same as in section 3.1.3, they have to define themselves criteria in order to determine on which occurrence they will send the request. In the present section, those internally defined criteria should take into account the fact that they would in principle not be in a position to decide about rejecting the transfer or executing it as long as they will not have received the answer to the request for complete /meaningful information.

[2] FIU = Financial Intelligence Unit

34. The request for complete/meaningful information should include a deadline for the PSP of the payer to answer. A maximum deadline should be set, such as 3 working days, or longer for payments from outside the EEA. However, PSPs of payees may decide to fix a shorter deadline. This deadline could be communicated through its insertion in the Terms and Conditions of the receiving PSP.

35. Once the PSP has sent its request for complete /meaningful information, it has to wait for its selected deadline, such as 3 working days, for receiving the requested information to run out.

36. Then, if it receives a satisfactory answer to the request for complete information, it should assess the suspicious character and, after having completed this assessment, decide whether to execute the transfer, reject the transfer or sending a STR to the FIU and holding the funds.

37. The PSP has to define policies and set up procedures and processes in order to complete an appropriate follow up to its requests for complete /meaningful information. This should in particular define its reaction to the absence of a valid answer in the required deadline and the processes for sending reminders to failing PSPs. In addition, the PSP should be able to demonstrate to its supervisor that those policies, processes and procedures are adequate in order to fulfil their objectives and are effectively applied.

38. For example, if it does not receive a satisfactory answer to the request for complete /meaningful information, it should proceed to the follow up to the request. This follow up could consist of sending a reminder, such as 3 working days after the first deadline has run out. The reminder should set a deadline for the sending PSP, which could be again 3 working days. The reminder could also notify that the sending PSP, in case it will not answer satisfactory within the deadline, will in future be subject to the internal high risk monitoring (cf. above 2.2.) and treated under the conditions of

Art. 9 (2) of Regulation 1781/2006. Another alternative could be that the PSP may choose to state this in its Terms and Conditions.

39. Additionally, the reminder should indicate that the respective transfer is currently pending. After that the deadline included in the reminder has run out, and whether or not it has received a satisfactory answer to its reminder, the receiving PSP should assess the suspicious character and, after having completed this assessment, decide whether to execute the transfer, reject the transfer or send a STR to the FIU and hold the funds. When it decides to execute the transfer, it has to take into account the factors that led him to hold the funds at the initial stage. For more details on *"Assessing the suspicious character",* refer to section 3.1.3.

3.2 The PSP becomes aware that a transfer is incomplete after having executed the transfer

40. Where the PSP of the payee becomes aware subsequent to processing the payment that it contained meaningless or incomplete information either as a result of random checking or by any other way, it must:
    a. consider the incompleteness /meaninglessness of the information as a factor in assessing whether the transfer or any related transaction is suspicious and whether it must be reported to its FIU;
    b. consider asking for the complete /meaningful information to the PSP of the payer or, where appropriate, to the intermediary PSP. In this case, it shall also proceed to the follow up actions to the request, as above mentioned.

4. Common understanding on Article 9 §2

4.1 The regularity of failure

41. Recital 17 calls for a common approach on Article 9 §2, which provides that PSPs have to react towards PSPs that are regularly failing to supply the complete information.

42. However, the Regulation does not elaborate on the concept of regularity. A common approach on this point will be highly desirable as a common response by EU PSPs will enhance the credibility and effectiveness of their reaction and, thereby, international compliance with FATF Special Recommendation VII, SR VII. The PSP of the payee shall determine when the other PSP is regularly failing. This could be due to different reasons, for example regularly not inserting the full information of the payer and/or regularly not responding to requests in a timely manner. Also the level of failure may vary according to the risk based approach of the payee PSP.

43. Accordingly the PSP of the payee shall consider what criteria determine whether the PSP of the payer has regularly failed to provide the required information. Until the PSP of the payee, has sufficient data to analyse its own experience in identifying such 'failure", the following criteria could, for example, be used:

a. the level of cooperation of the PSP of the payer relating to requests for complete/meaningful information sent ;
b. a threshold defined in a percentage of incomplete transfers or transfers with meaningless information sent by a specific PSP;
c. a threshold defined in a percentage of still incomplete transfers in a period or with meaningless information, after that the PSP of the payer has received a certain amount of requests for complete/meaningful information;

d. a threshold defined equating to an absolute number of incomplete transfers or transfers with meaningless information sent by a specific PSP; and
e. a threshold defined equating to an absolute number of still incomplete transfers or transfers with meaningless information in a defined period, after that the PSP of the payer has received a certain amount of requests for complete/meaningful information.

4.2 Steps to be taken

44. Once a PSP has been assessed as regularly failing by a PSP of a payee, the PSP of the payee should issue a warning to the PSP which is failing, in order to draw its attention to the fact that, in accordance with the present common understanding, it has been identified as regularly failing.

4.3 Transmission to the authorities

45. As provided by Article 9§2, once a PSP has been identified as being regularly failing to provide the required information, the PSP of the payee shall report that fact to the "authorities responsible for combating money laundering or terrorist financing". Determination of such "authorities responsible" remains within national arrangements, and they should receive this information. These "authorities" are encouraged to exchange the information with their national supervisors.

46. This transmission of such information should be clearly distinguished from a Suspicious Transaction Report, STR. Indeed, the purpose of this transmission is to signal that a specific PSP meets the criteria defining the regular failure in this common understanding, which indicates a difficulty to comply with SR VII. This transmission does not imply that the PSP of the payer is suspected of money laundering or terrorism financing. It implies that it might be failing to respect its obligations under SR VII. Some countries have chosen to develop a specific format for "Article 9 §2

reporting". This seems to enhance the perception of this distinction by PSPs.

4.4 Decision as to restrict or terminate the business relationship with a PSP reported as being regularly failing

47. The Regulation states that the PSP of the payee decides whether or not to restrict or terminate its business relationship with regularly failing PSPs.

48. For the PSP of the payee to act alone against a failing PSP may prove commercially disruptive, particularly where that PSP is an important counterparty.

49. In addition, we would also expect supervisors to share views about failing PSPs and consider what action they may take.

50. It should be stressed that, when the regularly failing PSP is also a correspondent bank from a third country, the decision taken according to the present section and the enhanced due diligence performed according to Article 13 §3 of the Third Anti Money Laundering Directive could all be included as part of the process of managing the cross-border correspondent bank's relationship.

5. Internal data collecting and reporting

51. PSPs should be able to demonstrate to their supervisory authority that there are effective policies and procedures in place related to data collection and internal reporting that are appropriate to meeting the requirements of the Regulation. Further, PSPs' internal control and audit policies and procedures for Anti Money Laundering and Combat of Financing of Terrorism should be subject to appropriate senior management oversight.

6. Threshold

52. It should be born in mind, when applying the Regulation and the present common understanding, that some countries outside the EU may have framed their own Regulation to incorporate a threshold of €/US$ 1,000 below which the provision of complete information on out-going payments is not required. This is permitted by the Interpretative Note to SR VII. This does not preclude European PSPs from calling for the complete information where it has not been provided. The existence of such a threshold, although relevant for the risk-based decision whether to carry out, to hold or to reject the transaction as well as for the determination of the regularity of failures, does not exclude the application of the procedures under points 3 and 4 above.

53. Any threshold of a higher amount would be non compliant with the SR VII and any related transfer will have to be considered as incomplete.

7. Review of the common understanding

54. Considering the fact that the common understanding takes into account the current level of compliance with SR VII at international level and the current functioning of payment, settlement, and supporting systems, it should be revised subject to the compliance level attained by the Industry with the regulations, and not later than when the Regulation 1781/2006 is reviewed.

Annex 1

Existing industry practice

This annex describes some existing practice that our liaison with the financial services industry has identified. It outlines some measures that are currently being employed by payment service providers.

- Bank N is a large bank based in an EU member state. It handles tens of thousands of electronic transfers every day. It sends and receives payments between EU member states, and countries outside of the EU, using the SWIFT message system. The SWIFT system prevents messages with blank fields from being processed. However, meaningless data can still be attached to payments: the SWIFT messaging systems are not able to prevent this. As such, Bank N undertakes post-event sampling of incoming payments traffic to identify where data is likely to be incomplete or meaningless. Sampling is focused on certain areas that are regarded to present a higher risk. Examples of higher-risk payments identified by Bank N include a) those that originate from payment service providers outside the EU, particularly those from jurisdictions that the bank has identified to be of a higher risk b) those from payment service providers that have previously failed to meet their obligations and c) payments that are collected by the payee in cash on a "pay on application and identification basis".

- Bank P is a small private bank based in a European capital that predominantly deals with customers from certain countries outside the EU. It receives very few electronic payments on behalf of its customers. When these payments are received it is not unusual for these to have originated from outside the EU, and to represent large sums of money. Bank P is able to subject each payment to scrutiny by a member of staff. The staff member's knowledge of the countries in question allows

them to quickly identify where, for example, the payer's address appear to not correspond with what might be expected.

- Bank Q is a medium-sized bank in an EU state. Bank Q seeks to identify incorrect data by performing post-event sample checks. As such, the payment has already been made by the time that Bank Q has become aware that information is incorrect. Aside from the practical issues, Bank Q is unsure whether it would be desirable to reject a transaction "in-flight": this could lead to civil claims for breach of contract, and also risk prosecution under national legislation that outlaws "tipping off" criminals. The next step that the bank takes is to seek complete information on the payer. It also considers whether there is anything suspicious about the transaction, although it is difficult to form suspicions based on this information alone. Bank Q is recording where payment service providers are failing to provide information, and considering which institutions are being sufficiently unreliable or unco-operative to warrant further action. Bank Q has not ruled out ending relationships with some payment service providers outside of the EU.

- For intermediaries, many view that the Payee PSP should address a request for missing information direct to the Payer PSP. It should not be necessary to involve the intermediary PSP, other than on occasions where their help is needed to provide a payer PSP transaction reference number in order to trace the payment.

- Some banks view that is sufficient to have information in Field 20 in the Swift standard message and that this meets the obligation according to the Regulation for a “unique identifier”. However, in non EU payments there must be information on the banks account in Field 50 in the Swift message.

Annex 2

Summary of Industry workshop on Anti Money Laundering in relation to the European regulation on the information on the payer accompanying funds transfers

London, 9th January 2008

1. A workshop was held with industry participants and the Anti Money Laundering Task Force ("AMLTF") on obligations imposed by the EU Regulation 1781/2006, implemented in December 2007. The AMLTF Chair, Andrea Enria, Secretary General of CEBS, provided background on the AMLTF, which was established in the second half of 2006 by CEBS, CESR and CEIOPS (- the three Level Three committees, 3L3), with a view to providing a supervisory contribution in anti-money laundering (AML) and Counter Terrorism Finance issues, with a specific focus on the Third Anti-Money Laundering Directive. In particular, its mandate is focused on the developments of risk-based approaches to Customer Due Diligence (CDD) and the "know your customer principle" (KYC) and their impact on the internal organisation and controls of intermediaries. The AMLTF provides a forum for exchange of experiences and networking between supervisory authorities, to help identifying practical issues that supervisors face in their day-to-day work and, when possible find common practical answers.
2. The workshop had been convened as the AMLTF wishes to find practical solutions to deal with payments that lack the required information in respect of the Regulation 1781/2006.
3. Further the Committee for the Prevention of Money Laundering and Terrorist Financing (CPMLTF), chaired by the European Commission and comprises of representatives from all Member States, asked the AMLTF to work on this topic, interacting with market participants. Also, the Commission is ensuring appropriate contacts with the bodies working on payments issues too.
4. The CBFA AMLTF member presented the AMLTF's (draft) paper AMLTF 2007 22 rev2, relating to information on the payer of accompanying

fund transfers to payment service providers of payees, and sought to gather industry views on the nature and relevance of the problem, to assist in AMLTF finalising this paper and discussing the issues at the CPLMTF. In particular the CBFA AMLTF member presented issues relating to the general principles for common understanding on Articles 8, 9, 10 and 16 of Reg. 1781/2006. In adherence to standard 3L3 practices for public consultation, the AMLTF intends to finalise this paper, and subject it to formal consultation, and hence workshop attendees' comments were sought informally on the current draft.

5. Discussion focussed on incomplete incoming transactions messages, both inter EEA and from 3rd countries. Market participants agreed that the problem is indeed relevant and expressed their availability to provide information on the amount and distribution (including, in terms of country of origin and Payment Service Providers) of the transactions with incomplete information.
6. The industry representatives also presented their approaches to dealing with the issue. Some differences emerged both in the timing of the assessment of the completeness of information as per Art 9.1 and in the interpretation of Art 9.2. An issue relating to Art 6 was also raised, calling for further investigation: it was pointed out that a reference number might be sufficient for funds transfer inter EEA, yet from a practical perspective, might not be sufficient for many competent authorities, in relation to their domestic AML/financial crime requirements.
7. Some concerns were expressed as to the compliance burden of some of the options presented in the draft AMLTF paper (i.e. under Art 9.1 and Art 10) where the AMLTF proposed i) PSP execute the transfer first and then ask for complete information. PSP wait for deadline for receiving the complete information to run out and then assess the suspicious character of the transaction; and ii) PSP define risk criteria in order to allow their systems to distinguish between those incomplete transfers that can be executed before assessing their suspicious character and those incomplete transfers for which the assessment of their suspicious character and the request for complete information should be done

before executing the transfer. Some also suggested that there may be an additional option, or that a mix of options should be sought that better reflects current market practices.

8. Although the urgency of the subject matter was acknowledged, several market participants invited the AMLTF not to rush to conclusions, especially in some areas.
9. The AMLTF Chair committed to come back to the industry group with:
    a. a request for some information by early February, and
    b. to submit, for an informal feedback, a revised version of the paper as soon as available; and
10. Further in adherence to standard 3L3 practices for public consultation, the AMLTF aims to subject its proposals for a 3 month public consultation, relatively soon, although there may be more flexibility in the consultation period so as to respect the urgency of finding a solution to the problem, having taken into account the informal pre consultation with industry.

ANNEX VI

Useful websites concerning the fight against money laundering and terrorist financing

Basel Committee website

www.bis.org

- Customer due diligence for banks October 2001;
- General Guide to Account Opening and Customer Identification February 2003.

Financial Action Task Force (FATF) website :

www.fatf-gafi.org

- The FATF website contains important information and documents containing details on the methods and techniques and the risks as regards the fight against money laundering and terrorist financing.